TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ 2,00 €
SOLO INFORMAZIONE E ARTICOLI

HACKER JOURNAL

n.161

www.hackerjournal.it



ATTACCO AL BIG BANG

Cronaca dell'ATTACCO all'ACCELERATORE

SUBME

Il CONTROLLO REMOTO diventa Trojan

RAM SOTTO GHIACCIO

Come RUBARE LE PASSWORD attraverso la RAM

ADSL SOTTO CONTROLLO

Scopri QUANTO TI PROMETTONO e QUANTO TI DANNO DAVVERO

QUATTORD. ANNO 8 - N°161 - 9/22 OTTOBRE 2008 - € 2,00

WLF PUBLISHING

Anno 8 – N.161
9 / 22ottobre 2008

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata
al Tribunale di Milano
il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Piccoli surfer crescono... **forse!!!**

"Si può dire civiltà un cannibale che mangia con le posate"
Anonimo

Grande scalpore ha gettato tra la comunità dei benpensanti e dei guardoni della rete la notizia secondo la quale il porno sarebbe ormai stato battuto!!!

Spieghiamo meglio, secondo le ultimi analisi effettuate sulla navigazione in rete i siti di social networking avrebbero surclassato come accessi i siti dedicati alla pornografia e anche gli studi fatti sulle parole più cercate attraverso i motori di ricerca darebbero risultati analoghi.

Dobbiamo forse credere che dopo decenni di leadership il "sesso" non spopoli più tra gli utenti della rete??? Dobbiamo pensare che una miriade di piccoli pornografi si siano convertiti ad altro??? E poi a cosa??? Le prime due domande non hanno risposta mentre quest'ultima si, come abbiamo visto, il web 2.0 spopola.



Secondo alcuni analisti della rete i giovani (americani, visto che l'analisi è stata compiuta lì) passano così tanto tempo tra Facebook, MySpace, YouTube e siti analoghi da non averne più per navigare su siti con materiale per adulti.

Potremmo essere molto soddisfatti di questo, finalmente si toglierebbe quell'alone morboso che circonda chiunque passi le sue nottate davanti al monitor facendo preoccupare i genitori per le sue diottrie, ma in realtà vedo (mio modestissimo parere) poca evoluzione in questo passaggio.

Da una popolazione che guarda altri fare sesso rischiamo di passare ad una popolazione che guarda gli altri e basta, con ancora più frustrazione, con intenzioni ancora più morbose, con uno spirito voyeuristico ancora più acceso.

Non voglio demonizzare il web 2.0 ma non crediamo che sia il paradiso, si possono passare ore facendosi bellamente i ca...voli degli altri, leggendo cosa gli scrivono gli amici, cosa fa, cosa dice, chi frequenta con buona pace della privacy. Si rischia di diventare tutti stalker virtuali e onestamente non credo che questo sia un gran passo avanti.

BigG

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Il futuro della musica digitale



:: CD addio!!!

Da un po' se ne parla e sembra ormai arrivato davvero il momento. SanDisk ha difatti annunciato la commercializzazione, con EMI Music, Sony BMG, Universal Music Group e Warner Music Group, di musica digitale priva di DRM in un nuovo formato, una micro-Sd card. La card sarà precaricata con brani degli artisti del momento delle major e, negli USA, sarà messa in vendita per le feste di Natale anche in grandi catene come BerstBuy e Wal-Mart. Il nome del nuovo supporto sarà "Slot-Music" e avrà la capacità fino a 1Gb e un costo tra i 7 e i 10 dollari.

:: L'Europa boccia Sarkozy

Ebbene si, il famigerato e temutissimo Pacchetto Telecom, in approvazione presso l'Unione Europea, è stato depurato da tutta quella parte che accoglieva la linea dettata dalla Francia in materia di anti-P2P. Come ricorderete si trattava di una serie di norme come il metodo dei tre avvisi prima della sconnessione definitiva dalla rete, piuttosto che l'utilizzo dei provider in veste di cyberpoliziotti, che Sarkozy e soci hanno già imposto in Francia e volevano vedere applicate anche nel resto d'Europa essendo, secondo loro, l'unico modo per frenare il fenomeno del filesharing. Grazie a Dio qualcuno presso l'Unione Europea si ricorda di essere stato eletto dalla gente e che dovrebbe lavorare al suo servizio e non al servizio delle Major e quindi questo pacchetto di norme contro il P2P è stato decurtato dal Pacchetto Telecom, le motivazioni sono semplici e lampanti, privacy, libertà, neutralità della rete e tutte quelle cose che andiamo ripetendo ormai da tempo. Una particolare nota di merito vorremmo darla alla relatrice Catherine Trautmann, che in mail rivolta agli eurodeputati ha definito l'accesso alla Rete un diritto fondamentale dell'individuo: nessuno può esserne privato senza la decisione degli organi giudiziari. Come possiamo non essere d'accordo con lei...





LA NASA ALL'ASTA

La NASA mette all'asta circa 25 tra licenze, brevetti e diritti inerenti alle nuove tecnologie. A rendere ciò possibile è una partnership tra il Goddard Space Flight Center e Ocean Tomo azienda specializzata nella vendita e nella promozione di beni intangibili. L'iniziativa è volta a commercializzare la tecnologia, per renderla fruibile al mercato pubblico, favorendone lo sviluppo. In ballo molti interessi, soprattutto tra le grandi aziende produttrici di tecnologia, pronte ad investire capitali per assicurarsi i preziosi lotti.

MACOS X 10.5.5

Il passaggio di MacOs X dalla versione 10.5.4 alla 10.5.5, che avviene con l'update appena rilasciato,ha apportato molte modifiche, soprattutto debug, a Leopard. L'elenco delle migliorie è disponibile sul sito di Apple ed è sotto attento esame di tutti gli operatori della Mela non ha fatto eccezione e le varie correzioni apportate a Leopard, il cui elenco è disponibile sul sito di Apple, stanno venendo esaminate con attenzione.



Tra i miglioramenti si può segnalare il rinnovo di iCal, che ora gestisce meglio gli eventi che devono ripetersi e si sincronizza più facilmente con iPhone, la sistemazione del bug che faceva avviare alcuni Mac ogni giorno alla stessa ora, che l'utente lo volesse o meno, e una più efficiente gestione del protocollo Imap da parte di Mail.

PAGARE LE FATTURE CON PAYPAL

Grazie a un accordo con OB10.com uno dei maggiori hub europei di fatturazione elettronica, è ora possibile pagare fatture elettroniche con PayPal, cliccando un bottone inserito nel file PDF della fattura. L'annuncio, che posiziona PayPal, oltre che come servizio B2C utile ai privati per pagare gli acquisti su internet, anche come servizio B2B (business-to-business) utile alle (piccole) imprese per pagare i fornitori, potrebbe cambiare il mercato della fatturazione elettronica. La fatturazione elettronica presenta due vantaggi principali, cui corrispondono due diverse visioni dell'offerta di servizi di fatturazione elettronica.
Il primo vantaggio è che permette di rendere meno laborioso per il ricevente il processo di autorizzazione al pagamento delle fatture. Il secondo vantaggio è che rende più efficiente l'effettuazione del pagamento e permette di offrire servizi finanziari (ad esempio l'anticipo fatture) in modo più semplice e sicuro.



FALLE CRITICHE

La lista di correzioni che Microsoft ha rilasciato questo mese comprende quattro bollettini che coprono vulnerabilità tutte definite critiche ma che non erano note precedentemente.
A essere aggiornati sono innanzitutto Media Player 11 che senza la patch può permettere l'esecuzione di codice malevolo da remoto e il suo codec Windows Media Encoder 9, che comporta lo stesso rischio.Soffrono poi di problemi analoghi - ossia l'esecuzione di codice da remoto - sia tutte le versioni di Windows supportate che Microsoft Office, nelle versioni 2003 e 2007 per Windows e nelle versioni 2004 e 2008 per Macintosh.

CHROME AGGIORNATO

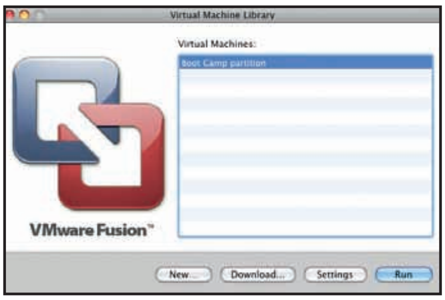
Tramite il servizio di aggiornamento automatico integrato in Chrome, Google ha rilasciato un aggiornamento del proprio brow-



HOT NEWS

ARRIVA FUSION 2.0

Palo Alto (USA) - Dopo un lungo periodo di beta testing, VMware ha lanciato l'attesa versione 2.0 del proprio software di virtualizzazione per Mac: Fusion. Rispetto alla versione 1.1, Fusion migliora il supporto alla grafica 3D e alle librerie DirectX 9.0, che ora è in grado di utilizzare in accoppiata alla specifica Shader Model 2. L'attuale versione 1.1 manca invece del supporto ai pixel shader, una caratteristica che limita pesantemente la compatibilità di Fusion con i giochi basati su DirectX 9.





16 CPU NEL NUOVO CX1

È CX1 il sistema con profilo 7U capace di accogliere fino ad otto schede madre con uno o due processori Xeon, per un massimo di 16 CPU. Il supercomputer "desktop" di Cray, che non necessita di appositi locali né di costosi sistemi di refrigerazione esterni, parte da un prezzo di 25mila dollari per arrivare, con le configurazioni più pompate, a sfiorare i 100mila dollari. Si rivolge soprattutto a quelle aziende che, pur necessitando di una discreta potenza di calcolo centralizzata, non necessitano o non possono permettersi un supercomputer "full size", il cui costo può arrivare a diversi milioni di dollari.



MICROSOFT NELLE SCUOLE

ANP, Associazione Nazionale dei dirigenti e delle alte Professionalità della scuola, ha siglato con Microsoft un protocollo d'intesa per l'aggiornamento dei propri iscritti alle novità introdotte da Internet e dalla società digitale. Obiettivo del protocollo, si legge in una nota, è quello di sviluppare congiuntamente iniziative di formazione rivolte al personale della scuola nel campo delle tecnologie dell'informazione e della comunicazione, con l'obiettivo di fornire ai dirigenti scolastici tutti gli strumenti educativi e formativi necessari a responsabilizzare docenti, studenti e genitori.



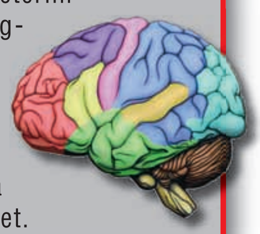
ser, che resta comunque in versione beta. L'update serve a risolvere tre problemi, il primo dei quali riguarda alcune vulnerabilità di sicurezza su cui però non sono stati rilasciati ulteriori dettagli.

A un altro bug era dovuto l'errato comportamento di Chrome che andava in crash se l'indirizzo di una pagina web conteneva il simbolo di percentuale; l'ultimo problema riguardava una cattiva gestione dei Javascript con Facebook.

IN CARCERE PER UNO SCANNER CELEBRALE

Di brain scanning si è parlato in diverse occasioni, ma in India qualcuno pare convinto che una particolare versione dello scanner cerebrale funzioni, anche in assenza di prove scientifiche attendibili: lo scorso giugno, servendosi di un BEOS test, un magistrato ha ritenuto una donna effettivamente colpevole dell'uccisione dell'ex fidanzato e l'ha condannata al carcere a vita.

Il BEOS (Brain Electrical Oscillations Signature) test è un sistema sviluppato dal neurologo indiano Champadi Raman Mukundan: impiega un elettroencefalogramma per determinare se un dato soggetto ricorda specifici dettagli di un crimine, nel momento in cui questo viene letto ad alta voce, spiega Engadget.

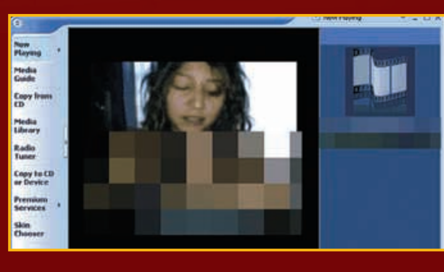




VIRUS PRESIDENZIALE

La campagna elettorale negli Stati Uniti è stata sfruttata come esca per diffondere l'ennesimo trojan

Le elezioni presidenziali negli Stati Uniti stanno attirando l'attenzione di tutto il mondo e i pirati informatici non potevano perdere l'occasione per sfruttare l'evento. L'ondata di spam che ha investito i computer americani riporta una falsa notizia riguardante il candidato democratico Barak Obama. Stando al testo del messaggio, il senatore sarebbe stato ripreso durante un "incontro" con alcune ragazze ucraine. La notizia è piuttosto improbabile, ma nel clima pre-elettorale è probabile che la curiosità degli elettori finisca per favorirne in ogni caso la circolazione.
Il file allegato al messaggio, in formato *.EXE*, visualizza effettivamente un video, nel quale ovviamente non compare mai Barak Obama. Durante la riproduzione del filmato, però, l'eseguibile installa sul computer il virus *Hupig-D*. Quest'ultimo è un trojan in circolazione da tempo, che permette al suo autore di sottrarre informazioni riservate dai PC colpiti.



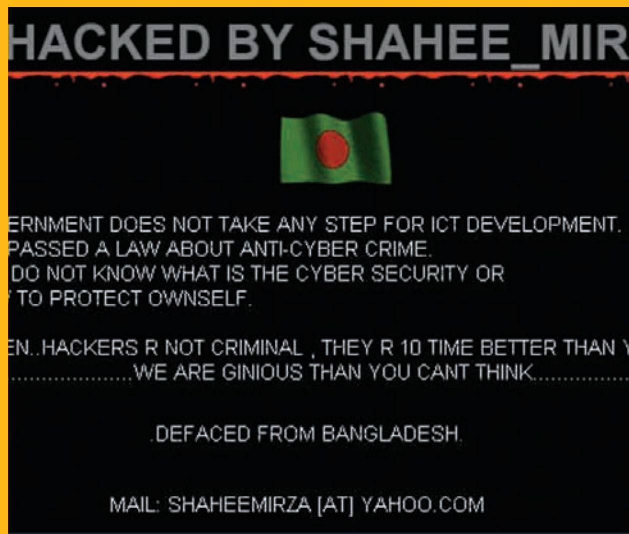
Per nascondere l''installazione, il virus visualizza un filmato "piccante". In background, però, installa il trojan.

IL VIRUS DEL MESE

Fino a qualche tempo fa, la sola idea di un virus per Linux sarebbe stata considerata come una burla. Oggi, purtroppo, le cose stanno diversamente. Linux/Rst-B è un virus in grado di colpire le machcine con sistema operative basato su Unix e creare una backdoor che permette all'autore di accedere al computer. La sua diffusione, rilevata dai laboratori Sophos ed evidenziata nella foto dai puntini rossi, ha raggiunto dimensioni preoccupanti.



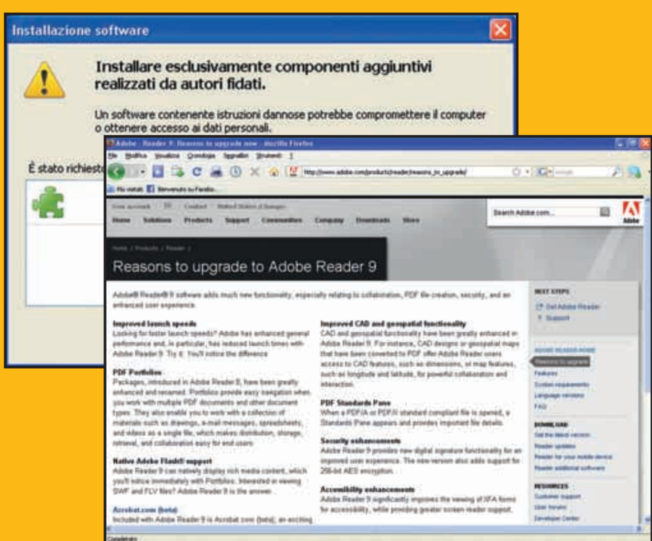
HACKER



Voleva criticare e politiche del suo paese, il Banlgadesh, attraverso un defacement, ovvero modificando la pagina iniziale di un sito governativo. Il giovane hacker, però,ha commesso un "piccolo" errore: ha inserito nella pagina il suo indirizzo di posta elettronica. La leggerezza gli è costata l'arresto, avvenuto nel giro di 24 ore, e un procedimento che potrebbe portarlo in carcere per 10 anni.

SICUREZZA

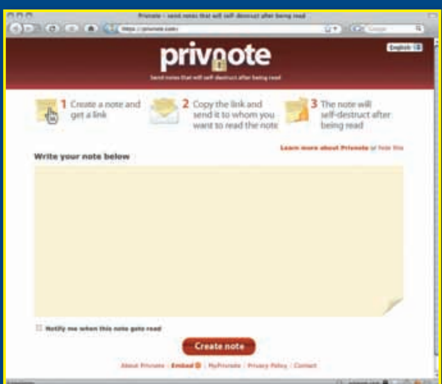
Nemmeno il più potente antivirus è in gradodi difenderci da tutte le possibili minacce che si annidano sul Web. Nel lavoro di tutti giorni, in definitiva, ciò che ci permette di evitare guai è il semplice buonsenso. Evitare di installare un'applicazione avviata da un Pop-Up, per esempio, è ormai considerato un comportamento "normale" e indispensabile per sottrarsi all'attacco di virus e spyware. Ogni tanto, però, il nostro bagaglio di esperienza deve esser aggiornato. È quanto succederà nei prossimi mesi con il formato PDF. I documenti creati con Adobe Acrobat sono spesso usati sul Web e, fino a oggi, li abbiamo sempre considerati inoffensivi. La nuova versione del software Adobe, però, è più potente e versatile, consente di inserire elementi attivi in Flash, documenti realizzati con altri software ed elementi attivi in grado di richiamare e trasmettere dati via Internet. Tutte le novità del programma sono descritte nella prova che troviamo questo mese nella rivista. Una cosa però è certa: i cari vecchi documenti di testo si sono trasformati in vere applicazioni, con tutti i vantaggi che ne conseguono in termini di potenzialità e i relativi svantaggi in termini di sicurezza. Il timore, infatti, è che i pirati informatici possano sfruttare le nuove funzioni per inserire virus e spyware all'interno dei file. Da domani, prima di aprire un qualsiasi documento PDF scaricato da un sito Web, sarà consigliabile eseguire una scansione completa del file usando il nostro fidato programma antivirus.



Questo messaggio si autodistruggerà...

Un'idea antica rimessa in pratica con un servizio moderno: aggirando le e-mail grazie al Web 2.0.

Uno strumento online per inviare informazioni riservate e messaggi "top secret". Si chiama Privnote (https://privnote.com/), ed il risultato del suo uso sono testi che spariscono dal server dopo la lettura.



Il segreto di Privnote è che non usa la posta elettronica ma fa rimanere nei confini del suo server tutte le comunicazioni, che sono pagine web che hanno il dono della discrezione. Interattivo ed accattivante quanto basta a rientrare nell'imperante "Web 2.0" Privnote non richiede un account né tantomeno vuole che si indichi destinatario o mittente: i messaggi si distribuiscono attraverso un semplice link che è la chiave (segreta) per leggere il contenuto.

:: E in pratica?

Privnote è rapido e immediato da usare a patto di avere un browser recente (Firefox dalla 2 in sù, ad esempio). È gratuito e senza alcuna registrazione o passaggio intermedio: appena caricato il sito è pronto all'uso e in alto mostra anche i tre passi chiave da seguire.

La prima cosa da fare è scrivere il testo nello spazio al centro della pagina.

Una volta fatto si può scegliere se avere anche una notifica di ricezione o meno: se si barra la casella verrà chiesto un indirizzo a cui mandarla e un riferimento (a piacere) ma nn è affatto necessario.

Il messaggio si "salva" con il pulsante rosso "Create Note" in fondo alla pagina: questo genera un url che va comunicato al destinatario.



Il link sarà del tipo https://privnote.com/n/carattericasuali e farà apparire nel browser il testo inviato insieme a due avvisi.



Il primo è che il testo originale è stato distrutto e che se lo si vuole salvare bisogna agire, ad esempio copiandolo, prima di chiudere la finestra e perderne quindi l'occasione.

Il secondo avviso è sulla crittografia usata che -secondo Privnote- fa in modo che solo mittente destinatario possono leggere il testo inviato (via https aggiungiamo noi) e che si declina ogni responsabilità sui contenuti trasmessi.

:: Quanto è sicuro

Il servizio ovviamente è meno sicuro di quello che afferma. Anche senza metterne alla prova la crittografia fino a che non si chiude la finestra del browser con il testo si può fare ciò che si vuole, copiarlo, stamparlo e anche uno screenshot, con buona pace di tutta la storia dell'autodistruzione. Detto questo Privnote può rivelarsi pratico e utile in casi in cui non si può o vuole lasciare traccia nella inbox e non sono in ballo segreti di stato: il servizio è facile da usare, rapidissimo e molto versatile visto il metodo usato: il link si può passare come e dove si vuole ad esempio via Instant Messaging e mantiene quel poco che promette.

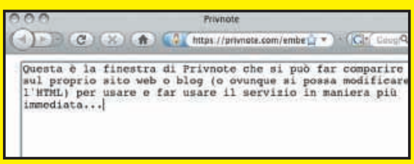
Nicola D'Agostino

ANCHE A DOMICILIO

Privnote offre la possibilità di usare il servizio direttamente da qualsiasi sito. In basso si trova un link all'embedding con la seguente riga da inserire nell'HTML di una pagina web:

<iframe src="https://privnote.com/embed/" style="width: 90%; height: 300px"></iframe>

Il risultato sarà una finestrella per digitare e creare il messaggio dal proprio blog o sito (o anche forum, fate voi) senza andare sul sito di Privnote.



CONTROLLO TOTALE

Privnote non è l'unico servizio a offrire un controllo totale (o quasi) sui messaggi di posta elettronica.



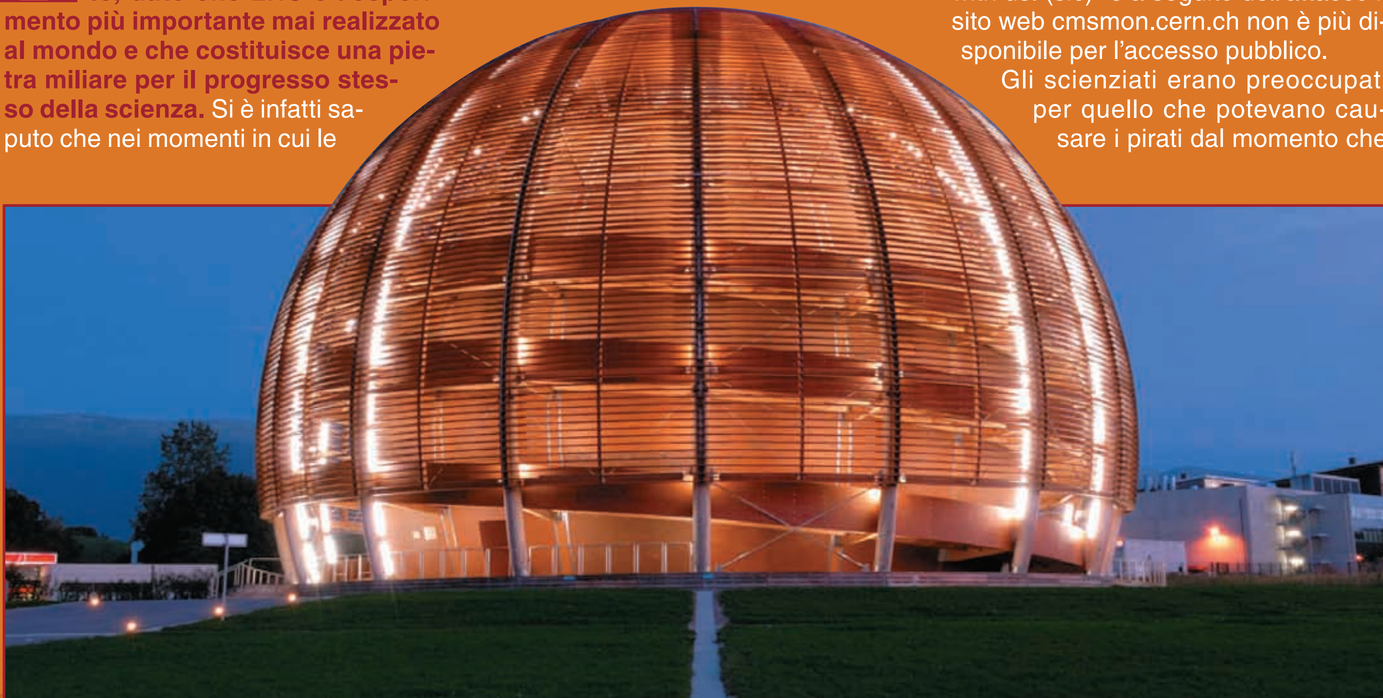
Il più interessante è Bigstring (http://www.bigstring.com/webmail/) che -secondo quanto si legge sul sito- promette una quantità enorme di cose. Impedisce copia e incolla, salvataggio e stampa dei messaggi e offre di poter eliminare o modificare il contenuto di un'e-mail dopo il suo invio oppure di distruggerla, allegati inclusi. Il servizio (che però richiede registrazione) non svela il metodo usato ma un indizio prezioso viene dal sorgente HTML dei messaggi giunti. A un'occhiata si nota che rimandano ad un file PNG sul server dell'azienda, tecnica che effettivamente permette il controllo quasi totale su cosa si può fare e -schermate a parte- di non lasciare alcuna traccia presso il destinatario.

Attacco al Big Bang

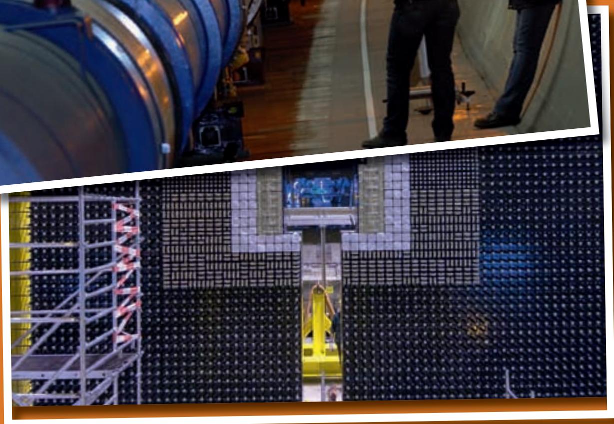
Proprio durante l'avvio del collaudo del Large Hadron Collider (LHC, l'enorme acceleratore di particelle installato al CERN di Ginevra) che teneva tutto il mondo col fiato sospeso, dei pirati informatici hanno realizzato un attacco che ha compromesso in parte la sua sicurezza

Tale attacco ha suscitato grande preoccupazione nella comunità scientifica mondiale, dato che LHC è l'esperimento più importante mai realizzato al mondo e che costituisce una pietra miliare per il progresso stesso della scienza. Si è infatti saputo che nei momenti in cui le prime particelle stavano già circolando nell'acceleratore, un gruppo di pirati informatici è riuscito a penetrare nel sistema e a visualizzare una pagina dal titolo "GST: Greek Security Team.", firmato come "We are 2600 - dont mess with us. (sic)" e a seguito dell'attacco il sito web cmsmon.cern.ch non è più disponibile per l'accesso pubblico.

Gli scienziati erano preoccupati per quello che potevano causare i pirati dal momento che







il pc compromesso si trovava poco oltre le difese di un PC di controllo di uno degli immensi rilevatori della macchina, un grandissimo magnete del peso di 12500 tonnellate, lungo 21 metri e largo 15. Nel caso in cui i pirati fossero riusciti a penetrare in un secondo computer del network, sarebbero stati in grado di spegnere alcune componenti del grande rilevatore che è stato davvero difficile far funzionare per l'esperimento. Fortunatamente solo un file è stato danneggiato, ma uno degli scienziati che abitualmente si occupa del CMS (Compact Muon Solenoid Experiment, uno dei quattro occhi dell'installazione che si occuperà di analizzare la pioggia radioattiva del Big Bang simulato) che si è trovato a fronteggiare i pirati ha ammesso che è stata un'esperienza da brividi.
"Sembra non ci sia stato alcun danno. Da quanto possono dire, è stato dimostrato che il CMS era insicuro", ha detto James Gillies, portavoce del CERN. "L'intrusione è stata rilevata velocemente perché abbiamo diversi livelli di network, un network per l'accesso generico e un network molto più sicuro per i dati sensibili nel quale opera LHC," ha detto Gillies. Il tentativo di intrusione è iniziato più o meno nel momento in cui l'enorme macchina stava iniziando a far circolare le prime particelle, sotto i riflettori dei media mondiali. Mercoledì pomeriggio, il mondo tratteneva il respiro mentre la macchina veniva innescata e intanto il team del CMS setacciava i computer rintracciando almeno una mezza dozzina di file caricati dai pirati tra il 9 e 10 settembre. "Pensiamo che qualcuno del Tevatron del Fermilab (l'acceleratore concorrente del LHC in America) abbia avuto i suoi dati d'accesso compromessi" ha detto uno degli scienziati che lavorano alla macchina. Quello che è successo non è stato nulla di eccezionale, serve solo a dimostrare che c'è sempre gente a caccia di prede."
Il team del CMS ha studiato con attenzione i file inseriti dai pirati prima di cancellarli, nel caso fosse stata installata una "backdoor" che permettesse un accesso in grado di superare i controlli di sicurezza. Il CERN conta su una strategia di "difesa in profondità", separando le reti di gestione e utilizzando diversi firewall e complesse password per proteggere i sistemi di controllo da software maliziosi, come attacchi di denial-of-service, botnet e macchine zombie che possono colpire con un attacco sincronizzato di centinaia di macchine sparse in tutto il mondo. E sono utilizzati oltre 110 diversi sistemi di controllo che monitorano, supervisionano e salvaguardano gli acceleratori, gli esperimenti e l'infrastruttura del CERN, per quanto riguarda gli edifici, l'erogazione di corrente elettrica e i sistemi di riscaldamento, fino al controllo d'accesso, la protezione dalle radiazioni e la sicurezza delle persone. Per migliorare i metodi della sicurezza è stato creato un gruppo di lavoro chiamato "Computing and Network Infrastructure for Controls". Un documento rilasciato dal gruppo dichiara "Gli eventi recenti mostrano che i problemi di sicurezza stanno diventando un serio problema anche al CERN." ma non ha rilasciato dichiarazioni relative alla sicurezza della struttura internazionale.





Pochi anni fa l'Università di Stanford in California annunciò che un certo numero di centri di calcolo ad alte prestazioni era stato attaccato da pirati informatici tentati dall'enorme potenza di calcolo del grid (un gruppo di macchine interconnesse ad alta velocità che elaborano i dati in parallelo). Oltre alla possibilità di poter spegnere le macchine, o rubare o cancellare dati, un uso malizioso di queste potenti macchine potrebbe consistere nel crack di password. Nel 2003, dei pirati penetrarono nello ScotGrid, un network di 150 macchine situato nell'Università di Glasgow. Intercettarono la password di un utente remoto che si collegava da Ginevra e lo usarono per avere accesso allo ScotGrid. Lanciarono anche degli script che provavano a riconfigurare le macchine per rubare altre password. E' possibile che ci siano dei collegamenti tra questi eventi e le autorità stanno indagando per scoprirlo.

Massimiliano Brasile





SOTTOMISSIONE...

In questo articolo analizzeremo "SubMe": un'efficace ed intuitivo programma che si sta facendo largo tra le numerose recensioni, commenti e critiche di blog e forum

Partiamo subito con il dire che il programma viene venduto sul sito http://www.subme.it (non è infatti un freeware) come software di gestione remota di uno o più computer. L'utilizzo che ne sta facendo la maggior parte degli utenti è però parecchio diverso: essi lo utilizzano infatti per accedere e conquistare il totale controllo via remoto di uno o più computer.

:: Analisi sistema

Tecnicamente il programma utilizza lo stesso sistema di tanti vecchi trojan e backdoor del passato quali: Back Orifice, Back Orifice 2000, Classer e NetBus. Il sistema è infatti basato su due file eseguibili "server.exe" e "client.exe" che comunicano tra loro grazie ad una precisa configurazione su determinate porte di ascolto/ricezione. Il primo file viene opportunamente configurato ed inviato al pc da "controllare" (via mail/messenger/cd/supporto USB..) mentre il secondo verrà eseguito sul pc dell'attaccante e permetterà di pilotare a piacimento il computer infettato (quello dove appunto risiede il file server.exe). Una volta avviato, il file "server" aprirà una porta di ascolto (o di invio nel caso in cui sia usato in modalità reverse [che vedremo più avanti]) per poter scambiare informazioni e comandi dal computer attacker.



:: Disclaimer

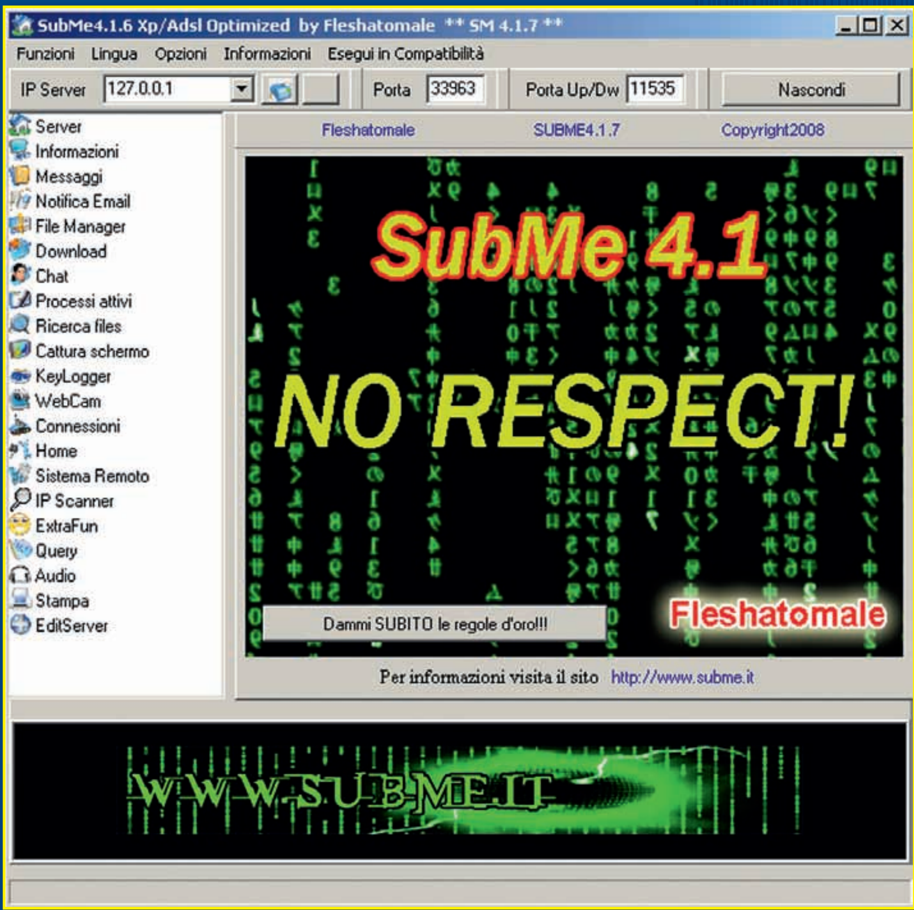
Usare un programma del genere solo per il gusto di divertirsi e devastare è un atteggiamento tipico dei lamer / script kiddies. Il mio intento è invece quello di stimolarvi a capire come possa funzionare un sistema del genere elencando le principali caratteristiche di questo software.

:: Analisi eseguibili

Partiamo dalla configurazione del file SERVER: tramite l'intuitivo menu si possono impostare password di accesso alla backdoor, porte di ascolto nonché altre comode features come la notifica di connessione dei pc controllati via posta elettronica. Una volta scelta la configurazione che ci interessa è bene salvare il file di SERVER e di inserirlo all'interno di un altro file es. video/foto/mp3, in modo da non insospettire gli utenti (e l'antivirus dei pc) a cui verrà inviato. Di norma viene infatti utilizzata una tecnica chiamata "joining" che permette di far visualizzare all'utente un file a nostra scelta es. video/foto/mp3 e di far avviare in maniera del tutto invisibile ("in background") il file di controllo. A questo punto non resta altro che inviare il file (con sorpresa all'interno) a qualche ignaro utente ed attendere che la nostra casella di posta elettronica si riempia di mail di notifica con indirizzi IP a cui collegarci.

Una volta ricevuta la notifica ci basterà aprire il file "CLIENT" e, una volta inseriti i dati di accesso al file di controllo, girovagare per il pc avendone il pieno controllo. Si possono visualizzare le





informazioni sull'hardware, versioni software, avere pieno accesso e controllo di dischi rigidi e supporti ottici (creare, modificare, cancellare file a nostro piacimento), visualizzare il desktop, loggare tutti i tasti digitati (keylogging di username, password etc...) modificare lo sfondo, aprire pagine web, visualizzare/terminare processi attivi , sbirciare nella webcam, far comparire messaggi di errore etc....

:: Reverse shell

Analizziamo ora la caratteristica più interessante di questo software: come potete vedere infatti sul sito ufficiale, "SubMe" viene venduto in due distinte versioni:

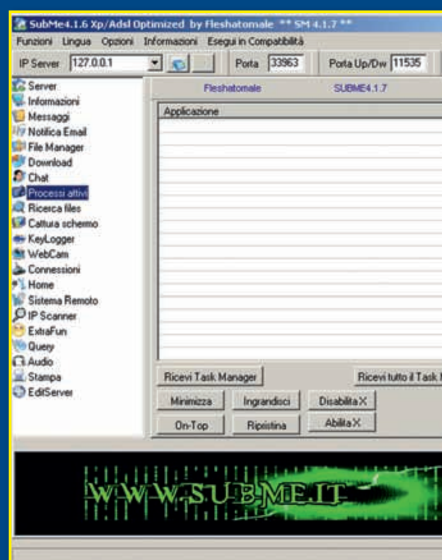
- 1 SubMe 4.1.7.
- 2 SubMe Rev3rse

La versione "Rev3rse" ha la peculiarità di utilizzare appunto una "reverse connection" in modo tale da riuscire a controllare anche pc che sono collegati a internet tramite rete locale LAN o con indirizzo "nattato".
WIKIPEDIA: "network address translation o NAT, ovvero traduzione degli indirizzi di rete, conosciuto anche come network masquerading, native address translation, è una tecnica che consiste nel modificare gli indirizzi IP dei pacchetti in transito su un sistema che agisce da router."
In parole povere tutti i computer collegati ad una rete "nattata" arrivano su internet con lo stesso indirizzo IP (che solitamente coincide con lo stesso IP del router) non consentendo quindi ad un pc remoto di stabilire una connessione diretta con la rete interna. Ciò è un problema se si vuole utilizzare un programma di gesione remota proprio perchè per fare in modo che la connessione vada a buon fine occorre effettuare un port-forwarding (in gergo viene chiamato "mappare" le porte del router) che è una cosa tutt'altro che facile da realizzare via remoto.

Si è riusciti però ad aggirare questo problema bypassando una delle regole di base del routing: dall'esterno infatti è difficile connettersi ad un pc della rete interna proprio grazie ai problemi che sono stati precedentemente descritti, al contrario, connettersi ad un pc di internet dalla rete interna è facile e veloce.

Proprio per questo la versione di "SubMe" chiamata "Rev3rse" sfrutta ciò per eludere firewall, router e geometrie della rete LAN. Il client attende una richiesta dai file server sparsi per i pc di ignari utenti e, una volta notificata la presenza acquisisce e stabilisce la connessione con essi.

Ricapitolando: nel caso di connessione standard il CLIENT (pc attacker) invia una richiesta al file SERVER (pc utente ignaro) per prendere il controllo del sistema. Nel secondo caso invece il file SERVER invia al CLIENT una notifica di connessione ed in caso affermativo la stabilisce.



:: Conclusioni

Sperò che questo articolo non vi incentivi ad utilizzare un software come questo senza capirne il funzionamento e usandolo per danneggiare qualcuno, quanto magari vi stimoli ad imparare, capire ed analizzare il funzionamento di molti interessanti programmi che sono oramai su tutta la rete. ■

Quant'è veloce la tua ADSL

Ottenere una buona connessione ADSL può essere una missione impegnativa: ecco come controllare il suo stato di salute



Un PC senza Internet è un po' come una moto senza ruote: potrebbe raggiungere ogni parte del globo e invece rimane inchiodato a casa nostra. È quindi indispensabile dotarsi almeno di una linea ADSL, anche se spesso può essere fonte più di dolori che di gioie. A dar retta alle varie pubblicità dei provider, infatti, si ha sempre l'impressione che la nostra linea sia infinitamente più lenta. In verità dietro ai numeri delle velocità nominali dichiarate dai vari fornitori si nasconde una situazione decisamente più modesta. La qualità di una linea ADSL dipende da numerosi fattori, alcuni dei quali non controllabili nemmeno dal provider che ci fornisce il servizio. Un primo passo possiamo però farlo noi stessi, mediante una serie di strumenti che Internet ci mette a disposizione per misurare la qualità della linea, le velocità di upload e download, i tempi di latenza e capire se il nostro provider sta davvero fornendo il miglior servizio possibile.

:: Come funziona

Tra i vari tipi di connessione a banda larga, quello che sfrutta la tecnologia ADSL è in assoluto il più diffuso. Come tutti i sistemi appartenenti alla famiglia DSL, ha il vantaggio di non richiedere una nuova infrastruttura: basta il comune cavo telefonico, il cosiddetto doppino, per accedere alla Rete. Il doppino, realizzato in rame, è in grado di portare più segnali contemporaneamente, purché questi viaggino a frequenze diverse. Basta quindi che i dispositivi collegati siano sintonizzati sulla frequenza opportuna per ricevere solo il segnale a loro dedicato. Il router collegato alla presa telefonica serve proprio a isolare le frequenze ADSL da quelle telefoniche, permettendo al telefono e al collegamento a Internet di funzionare contemporaneamente. Per come è ideato il sistema e

CONTROLLIAMO IL MODEM

Per verificare lo stato e la qualità del nostro collegamento ADSL, può essere insufficiente affidarsi ai soli programmi e servizi Web eseguibili direttamente dal PC. Queste soluzioni, infatti, possono misurare la qualità del segnale ricevuto solamente estrapolando i dati provenienti dal trasferimento. Ecco perché la maggior parte dei modem ADSL mettono a disposizione una serie di menu interni per verificare lo stato della connessione. Poiché il modem è fisicamente collegato alla linea, può effettuare misurazioni elettriche approfondite. I dati forniti variano molto a seconda del modello di modem, ma uno piuttosto importante è il Rapporto segnale/rumore o Signal/noise ratio. Questo valore è espresso in Decibel e indica la qualità del segnale. Un numero più elevato indica un segnale più pulito, esente da disturbi.





per i principi fisici che sfrutta, si intuisce facilmente che ogni trasmissione può essere condizionata da elementi come la potenza del segnale, la qualità del cavo, i disturbi generati da altri dispositivi. Tutti questi fattori contribuiscono a modificare la qualità della nostra linea ADSL, di solito in peggio rispetto a quanto promesso dal provider. Le velocità nominali indicate nelle varie promozioni, infatti, si riferiscono alla capacità teorica del cavo in condizioni ottimali. Condizioni, che, nemmeno a dirlo, si verificano molto di rado. Perché un trasferimento avvenga alla velocità massima sarebbe necessario un collegamento abbastanza vicino a una centrale, con un doppino nuovo, steso alla perfezione e perfettamente isolato.

:: Questione di fisica

Le principali cause dello scarso rendimento di una linea ADSL sono da ricercare nelle modalità di distribuzione. Lo sfruttamento della rete telefonica, infatti, ha messo in luce una serie di difetti e problemi che prima non si erano mai manifestati. Prima di tutto il livello di usura dei cavi telefonici, che contribuisce negativamente alla qualità del segnale. Poi la distribuzione delle centrali di smistamento, più che sufficienti per il traffico voce, ma inadeguate per quello dei dati. La velocità massima che possiamo ottenere dipende anche dalla distanza della nostra abitazione dalla centrale telefonica. I fornitori di servizi ci vendono la connessione sulla base della velocità di partenza del segnale, non quella di arrivo. Consideriamo che la velocità di accesso decade rapidamente e a 5 chilometri di distanza non può superare i 640 Kilobytes al secondo. Purtroppo è molto difficile conoscere la distanza dalla nostra centrale visto che questi dati sono pubblicati controvoglia da chi fornisce l'infrastruttura. Il problema della distanza, praticamente inesistente in città, diventa invece quasi drammatico nelle zone rurali, dove spesso una sola centrale fornisce più paesi impedendo di fatto la diffusione delle linee ADSL.

:: Scavando nella Rete

Usando a fondo la Rete e sfruttando servizi seminascosti, possiamo comunque risalire ai dati più segreti della nostra linea. Per iniziare, colleghiamoci all'indirizzo https://intra.eutelia.it/cgi-bin/wbc_slbverificacoperturaservizialargabandawhs. Inserendo il nostro numero di telefono possiamo sapere la denominazione della centrale a cui siamo collegati. Per individuarne l'indirizzo dobbiamo sfruttare un file risalente al 2004

UNA MARCIA IN PIU'

Dal mondo dei programmi Open Source arriva una pratica soluzione per tenere sotto controllo la nostra connessione ADSL. Se abbiamo installato il browser Firefox, www.getfirefox.com, possiamo sfruttare il versatile sistema di moduli aggiuntivi e aggiungere il Broadband Speed Test and Diagnostic 1.1 da https://addons.mozilla.org/it/firefox/addon/2360. Una volta installato possiamo raggiungere questa estensione dal menu Strumenti e usarla per controllare la nostra connessione in qualsiasi momento.



3 CONSIGLI PER MISURARE L'ADSL

Durante le prove, non utilizziamo altri programmi che sfruttano l'accesso a Internet: i risultati sarebbero sicuramente poco attendibili. Controlliamo anche che il computer non stia scaricando gli aggiornamenti automatici.

Ricorriamo a più di un servizio di prova dell'ADSL e consideriamo valido il valore medio. La velocità misurata, infatti, dipende anche dal tipo e dalla posizione del server utilizzato per la misurazione.

Misurare la velocità dell'ADSL nelle ore di punta per il traffico. Se siamo collegati in una zona di uffici, proviamo in orario di lavoro. In una zona residenziale proviamo la sera e nei fine settimana.

che circola in Rete. Facciamo una ricerca su Google con le parole Centrali ULL per CONSIP e scarichiamo il documento in formato Excel che troveremo. Con un po' di fortuna troveremo l'indirizzo della centrale e potremo calcolare la distanza sfruttando uno dei numerosi servizi di mappe online. Purtroppo la costruzione di nuove centrali telefoniche è molto costosa, quindi al momento ci dobbiamo rassegnare a quella che utilizziamo. La qualità del nostro collegamento ADSL dipende anche dall'affollamento della zona. Se nel luogo in cui abitiamo sono in molti a usare la banda larga, è possibile che le prestazioni siano piuttosto vicine alla banda minima garantita.

:: Proviamo la linea

Per verificare la velocità della nostra linea troviamo un bel po' di servizi online e alcuni programmi che si basano tutti sullo stesso principio: tramite un server di riferimento vengono effettuate alcune prove di trasferimento e, in base al tempo impiegato per inviare e ricevere i dati, viene calcolata la velocità effettiva della linea. Fra i servizi disponibili il più famoso è Speedtest.net, www.speedtest.net, che esegue alcune prove con un sistema di controllo grafico piuttosto originale. Scegliendo un server di riferimento dalla mappa, possiamo verificare la velocità della nostra linea. Questo sito mette a disposizione anche un Gadget in HTML per pubblicare i risultati del test sul nostro sito o blog. Se preferiamo un servizio più sobrio, possiamo affidarci a quello di DSLReports.com accessibile all'indirizzo http://www.dslreports.com/stest?loc=2, oppure http://www.bandwidthplace.com. Volendo possiamo anche includere uno strumento nel nostro sito sfruttando il servizio messo a disposizione da Audit my PC, http://www.auditmypc.com/speedtest.asp. In questo caso chiunque si collegherà alla nostra home page potrà effettuare un test di velocità della sua linea.

:: Kilobit e kilobyte

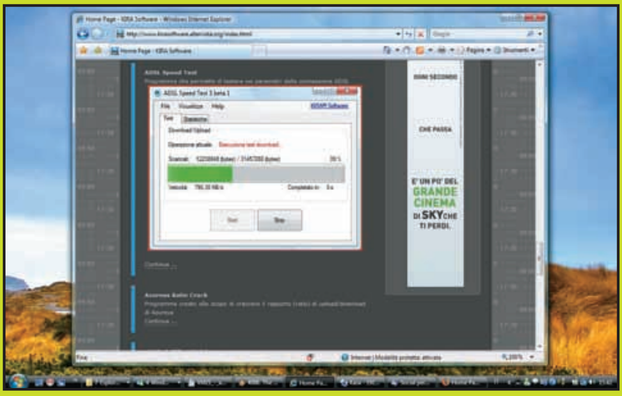
Eseguite tutte le prove che riteniamo opportune, possiamo confrontare i risultati ottenuti con i dati teorici della nostra ADSL. Il calcolo è semplice: se conosciamo la velocità in megabit al secondo, che di solito è quella con cui viene pubblicizzata la linea, dobbiamo moltiplicare il valore per 1.024 e dividere il risultato per 8 per ottenere la velocità in Kilobyte per secondo, valore normalmente usato per indicare la velocità di trasferimento. Ad esempio una linea a 7 Mega dovrebbe disporre di una velocità di download pari a 896 kilobyte per secondo. Se ci interessa anche la velocità di upload, facciamo attenzione: spesso è indicata in kilobit al secondo, per cui dobbiamo dividere il valore per 8 per ottenere i kilobyte al secondo.

:: Attenzione alla latenza

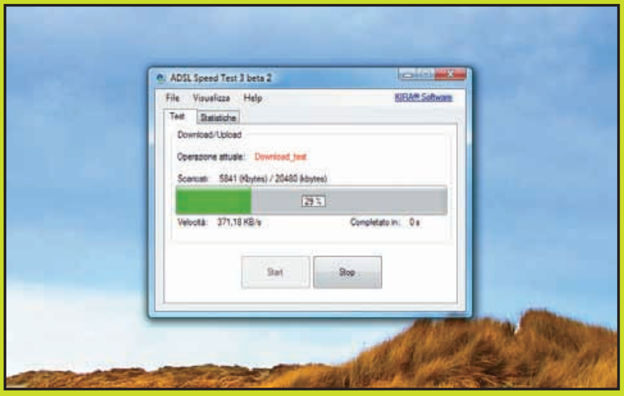
Oltre alla velocità di trasferimento, c'è un altro parametro interessante, soprattutto se siamo giochiamo online. Si tratta della latenza, ovvero del tempo di risposta della nostra linea, quello richiesto perché la nostra richiesta arrivi fino al server che ci interessa e torni indietro.

Questo valore, è espresso in millisecondi e chiamato ping. Minore è il valore migliore è la qualità della nostra linea. ■

ADSL SPEED TEST

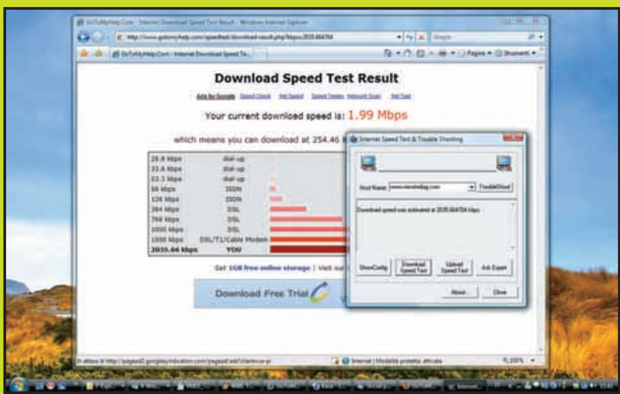


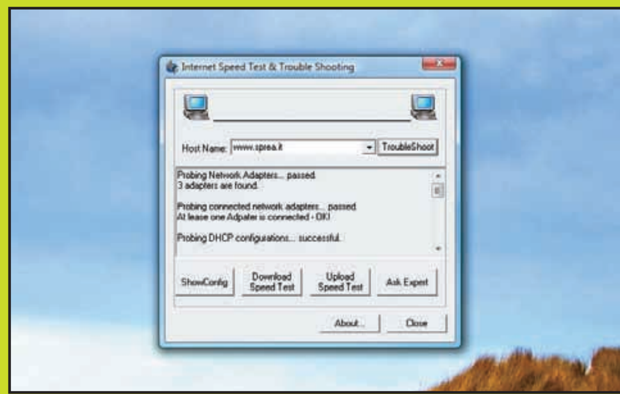
UN PROGRAMMA SPECIALIZZATO
Da www.kirasoftware.altervista.org possiamo scaricare l'ADSL Speed Test. È un piccolo programma senza installazione: estraiamo il file compresso e facciamo doppio clic sull'eseguibile.



AVVIO E CONTROLLO
ADSL Speed Test mostra una sola finestra. Facciamo clic su Start e aspettiamo il termine della prova sulla nostra linea ADSL. Nella scheda Statistiche troveremo poi tutti i risultati.

ANALISI APPROFONDITA





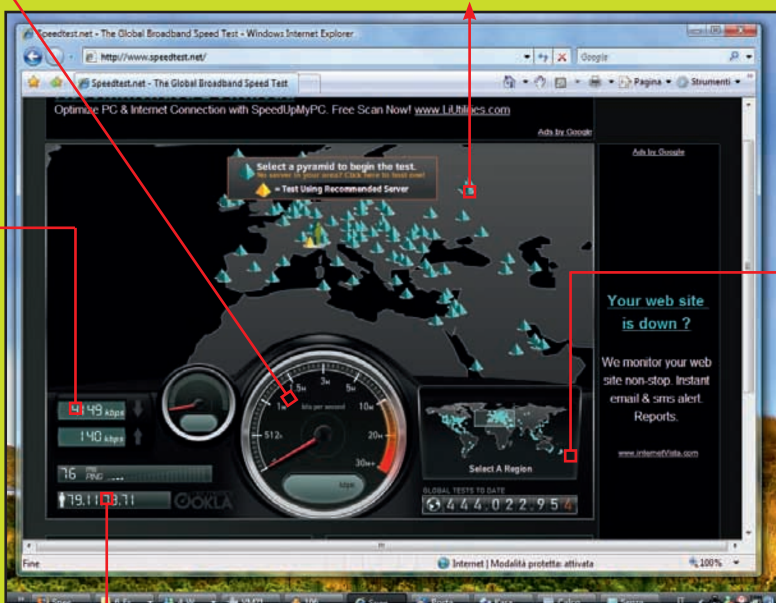
PROVE SEPARATE
Scarichiamo il programma scegliendo Speed Test and Diagnostics (Window Program) da www.dsl-speedtest.us, avviamolo e scegliamo uno dei test. Il risultato comparirà in una finestra del browser.

CONTROLLO
Speed Test and Diagnostics permette di controllare anche lo stato della connessione verso determinati siti Web. Scriviamo l'indirizzo e facciamo clic su Troubleshoot per controllare se tutto va bene.

COME MISURARE LA VELOCITÁ

COME IN AUTO
Ecco un modo simpatico per comunicare la velocità della linea durante la prova. Non lasciamoci condizionare dal tachimetro: i valori sono quelli espressi come numeri a lato.

SCEGLIAMO IL SERVER
Speedtest.net consiglia il server più vicino per eseguire la prova della tua linea ADSL. Possiamo comunque scegliere un altro server selezionando una delle piramidi.



ECCO LE VELOCITÀ
Una volta terminata la prova, qui troviamo la velocità effettiva del nostro collegamento espressa in kilobit per secondo. Dopo qualche istante si apre una finestra che ci illustra i risultati in modo più chiaro.

ESPLORIAMO IL MONDO
Se vogliamo verificare la velocità del flusso di dati verso una zona precisa del mondo, facciamo clic in questa mappa e spostiamo il piccolo rettangolo per visualizzare altri server sparsi per il globo.

IL NOSTRO INDIRIZZO IP
Il sistema di Speedtest.net rileva automaticamente l'indirizzo IP del PC che stiamo utilizzando. Tale indirizzo viene utilizzato per rilevare con esattezza il provider che fornisce l'accesso a Internet.

HABARI

PER UN BLOG MODERNO, SOLIDO E SICURO

Frustrati da WordPress? Delusi da Movable Type? Textpattern non vi convince? Trovate troppo complessi o sovradimensionati Drupal e Mambo/Joomla?

Volete un software di gestione contenuti online che sia aperto e libero, progettato con in mente la massima sicurezza possibile, che sia su misura per le esigenze di comunicazione e condivisione e che offra una gestione essenziale e tutt'altro che macchinosa? La risposta a questa domanda potrebbe essere Habari (http://habariproject.org/en/) un nuovo arrivato nel panorama dei CMS e software per curare blog. Vediamolo più da vicino e in azione.



La home page di Habari con in evidenza un filmato in Flash che ne mostra l'installazione e l'uso.

:: Funzionalità, protocolli aperti e sicurezza

Il manifesto di Habari è impressionante e spiega che il software è stato pensato e progettato per affrontare questioni pressanti come lo spam nei commenti e gli accessi enormi derivanti da segnalazioni su Digg e simili "di fabbrica" e non con aggiunte più o meno riuscite.
Tra le differenze con le altre soluzioni per blog e siti dinamici c'è la questione sicurezza: Habari proclama di adottare tecniche di programmazione ad oggetti e quindi di poter ridurre le vulnerabilità dei database, in particolare gli attacchi di SQL injection. Non guasta anche lo schierarsi a favore di protocolli aperti, standard e ben documentati, tra cui la scelta di Atom per i feed, saltando a piè pari il marasma di versioni di RSS.

:: Get Habari

Habari è ancora giovane e con parecchi aspetti da migliorare: il modo migliore per capire se fa al nostro caso è di scaricarlo ed installarlo. L'ultima versione "stabile" al momento in cui scriviamo è la 0.5 ma consigliamo di provare lo "snapshot", cioè la versione in corso di sviluppo in cui sono presenti nuove funzionalità e sono stati corretti diversi bug: entrambe sono disponibili dalla pagina dei download (http://habariproject.org/en/download) o direttamente nell'elenco http://habariproject.org/dist/ (lo snapshot è quello chiamato habari_head.zip).
I requisiti del server sono più o meno quelli standard per i CMS basati su PHP e database *SQL:
Apache (1.3.x, 2.x o superiori) con mod_rewrite abilitato o in alternativa Lighttpd o Nginx. Il database può essere MySQL 4.1.x o superiore oppure SQLite o PostgresSQL.La versione di PHP deve essere dalla 5.2 in sù con i moduli PHP Data Objects e driver per database scelto, SimpleXML, Hash, Iconv, Mbstring, Tokenizer e JSON.Per la cronaca tutti questi requisiti sono soddisfatti anche da un hosting a basso costo come Tophost (con il pacchetto base Topweb) ma se avete dubbi potete interrogare le caratteristiche con un file di test con estensione .PHP e all'interno questa semplice riga di codice:

```
<?php phpinfo() ?>
```

oppure interpellare l'assistenza del vostro provider di hosting.

:: Installazione

Sul wiki del sito di Habari (vedere la voce "Documentation" in alto) si trova l'installazione per filo e per segno con varianti e versione avanzata. Proviamo a sintetizzarla in pochi semplici passaggi.

0) Creare un nuovo database (noi abbiamo usato MySQL) e annotare l'indirizzo del server dove si trova, il nome utente, quello del database e la password.

1) Impostare la root della directory o home dove installerete Habari abilitandola in scrittura a chiunque (con chmod o+w). Alla fine della procedura questi permessi sono ovviamente da rimuovere (con
chmod o-w o i classici numeri).

2) Copiare il contenuto del file .zip scaricato o decomprimerlo direttamente sull'ftp.

3) Far partire l'installazione digitando l'indirizzo http://percorsoalvostrositodihabari se Habari è nella root oppure http://percosoalvostrosito/directorydihabari se è in una directory (in questo caso chiamata 'habari').

4) Compilare tutti i campi in "Installation" inserendo le informazioni del database (man mano che andate avanti il software verificherà le informazioni) e lasciare "Table Prefix" come è.



5) Se i dati sono corretti si passa a compilare i campi in "Site Configuration" dove si sceglie nome del sito, utente (tassativamente admin, in caso contrario si rischia di non accedere all'amministrazione), la password e l'e-mail per comunicazioni.



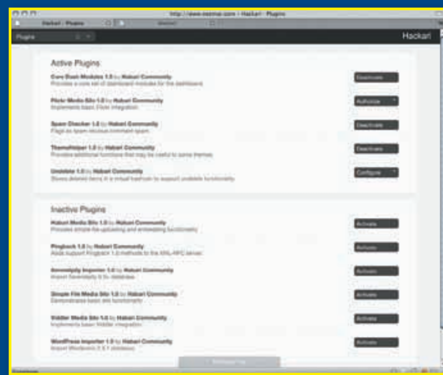
6) Se state usando una versione di prova potrebbe comparire una schermata con la scelta dei plugin da attivare.



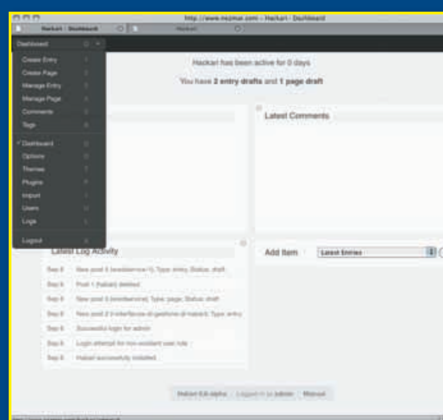
7) Un clic sul pulsante "Install Habari" ed abbiamo finito. Subito dopo verrà caricata la homepage con il post automatico di prova e non resta che fare login e personalizzare il sito o mettersi subito a scrivere.

:: Questione di interfaccia

Una volta installato Habari si trova un'interfaccia di amministrazione rinfrescante per la sua semplicità e chiarezza che aderisce a delle linee guida chiamate Monolith (http://wiki.habariproject.org/en/Monolith_Human_Interface_Guide): sia ben chiaro, le funzionalità non solo di base ci sono ma è stato fatto uno sforzo ben preciso per rendere ma gestione accessibile e il meno intrusiva possibile. Insomma: tante piccole attenzioni all'utente, come il raggruppamento visivo dei plugin in attivati e non attivati



Il pannello di controllo, il dashboard, poi è l'antitesi di quello delle versioni recenti di WordPress: pulito, essenziale e pilotabile anche da tastiera, con un menù sulla sinistra che si srotola e fornisce accesso a tutto ciò che serve, anche il logout.



Mostriamo infine la schermata per la scrittura dei testi, davvero notevole. Le opzioni e impostazioni ci sono ma sono "fuori dalle scatole": ci siamo solo noi e quanto vogliamo dire, scrivere e condividere.

Non vi viene voglia di provarlo subito questo Habari? ■

CHE VUOL DIRE HABARI?

Suona come giapponese ma in realtà è un termine tratto dal linguaggio africano (Ubuntu docet?) e vuol dire letteralmente "che novità ci sono?". In Swahili dire Habari equivale a chiedere "come va?". La risposta -in genere- sarà "nzuri sana" e cioè "molto bene", un buon auspicio per chi decide di dare fiducia a questo giovane ma promettente software.

Attacco di COLDBOOT



Siamo tranquilli e sereni con la nostra password sulla partizione di sistema e crediamo di essere inattaccabili, ma non è così...

Se si potesse stilare un'ipotetica classifica dei componenti che possono maggiormente compromettere l'integrità di un sistema, sicuramente la RAM potrebbe essere sul podio.
Già sfruttata durante il serial phishing e le operazioni di crack delle varie protezioni anticopia, la RAM ora presta il fianco ad un nuovo attacco in grado di ridurre notevolmente la sicurezza dei dati presenti su un PC. Il nuovo attacco prende il nome di cold boot e mira ad ottenere le chiavi di crittografia con cui alcuni dei più moderni programmi di sicurezza criptano i dati presenti sui dischi fissi dei computer, in particolar modo dei portatili. Il meccanismo alla base dei programmi di crittografia è piuttosto semplice. I dati vengono salvati in modo protetto e all'avvio vengono richieste una o più password che servono per decifrare le sezioni protette del disco. In mancanza di queste, i file o i dischi risultano illeggibili e non utilizzabili. Un attacco di forza bruta impiegherebbe troppo tempo per poter estrarre una chiave valida, soprattutto se la password scelta da chi ha protetto il disco è superiore alla lunghezza di 8 caratteri e strutturata seguendo gli accorgimenti minimi per renderla sicura. Un malintenzionato può sostituire l'attacco di forza bruta con uno di tipo cold boot. Per effettuare questa operazione è necessario poter disporre fisicamente della macchina da violare, anche se è possibile effettuare, in alcuni rari casi, l'attacco tramite procedure di boot PXE, ovvero attraverso la rete locale. Questa caratteristica rende i portatili più "deboli" visto che è possibile trasportarli e prelevarli con minore difficoltà.

:: Ricerca e attacchi

L'università di Princeton ha effettuato un esperimento eseguendo attacchi cold boot su vari PC con differenti marche di memoria RAM e con dischi protetti e crittografati da alcuni dei più diffusi programmi e i risultati sono stati sconcertanti. Quasi tutti i computer si sono rivelati vulnerabili e anche le memorie ECC non sono risultate esenti da questa falla di sicurezza, soprattutto quando è stato impedito loro di funzionare su un sistema adeguatamente configurato. All'indirizzo http://citp.princeton.edu/memory/ è possibile reperire i dettagli tecnici dell'esperimento e anche alcuni programmi in grado di effettuare il dump della memoria del computer bersaglio e l'estrazione dell'eventuale chiave rilevata. Alcuni

accorgimenti possono ridurre l'efficacia o la possibilità di un attacco cold boot, e tra questi prima fra tutti è la disabilitazione del boot da periferiche rimovibili e l'immissione di una password per la configurazione del BIOS del PC.



La memoria ram si occupa di trasferire e immagazzinare dati e riesce ad effettuare queste operazioni tramite semplici condensatori che memorizzano il valore di un bit 0 o 1. Quanto maggiore è la temperatura tanto più breve sarà il tempo richiesto da questi condensatori per scaricarsi



Per poter effettuare l'attacco cold boot avendo più tempo a disposizione è sufficiente raffreddare la memoria RAM del computer bersaglio in modo da poter conservare le informazioni più a lungo.

:: L'attacco vero e proprio.

Per effettuare correttamente un attacco cold boot sono sufficienti pochi accorgimenti. Prima di tutto è necessario disporre di una periferica USB da cui effettuare il boot dopo averla collegata sul computer bersaglio e su cui siano caricati i programmi per effettuare il dump della memoria RAM ed eventualmente l'estrazione della chiave DES o RSA. Una volta predisposta questa periferica è necessario procedere al riavvio della macchina tramite pulsante di reset oppure tramite interruzione dell'alimentazione o, nel caso di un computer portatile, eventuale rimozione della batteria. In questo modo si impedirà al software di rimuovere dalla memoria RAM eventuali chiavi o password memorizzate. All'accensione del computer sarà necessario specificare la nuova periferica di boot indicando il disco esterno USB oppure il boot di rete, ma in questo caso non è assicurata la riuscita dell'attacco. Le strade da percorrere sono due: il lavoro può essere effettuato direttamente sulla macchina bersaglio oppure, tramite rimozione e raffreddamento della memoria RAM installata su un nuovo computer opportunamente predisposto. In entrambi i casi sarà necessario effettuare il boot tramite un sistema esterno in modo da andare a scrivere meno dati possibili sulla memoria da leggere.

:: Seconda fase

Effettuato il boot e lanciato il programma di dump della memoria si avrà tutto il tempo necessario per poter effettuare la ricerca delle chiavi di cifratura degli hard disk tramite appositi programmi.
In alcuni rari casi la memoria si sarà cancellata in parte per cui sarà possibile estrapolare solo parti della chiave, che comunque potranno essere adoperate per effettuare ulteriori attacchi, ad esempio uno di forza bruta basato sui dati ricavati. Un pericolo secondario derivante da questo tipo di attacco è la possibilità di recuperare non solo le chiavi di cifratura degli hard disk, ma anche eventuali password o dati sensibili che al momento dello shutdown erano presenti in memoria. In questo caso la sicurezza dell'utente risulta totalmente compromessa. Non esistono contromisure che rendano completamente immuni i computer da questo genere di attacco, come sostengono sia l'università di Princeton sia Giuseppe Petrillo nel suo blog all'indirizzo http://glpetrillo.blogspot.com/2008/08/cold-boot-attack-violare-la-sicurezza.html, ma alcuni accorgimenti come il blocco del boot da periferiche esterne o eventuali password possono ridurre le possibilità di effettuare simili attacchi, misure definitive invece richiederanno tempo per modificare strutture hardware e procedure software di sicurezza.



Una volta estratta e raffreddata la memoria RAM conserverà i suoi dati per un tempo decisamente più lungo rispetto alle normali condizioni e l'attacco potrà svolgersi in totale tranquillità.

L'università di Princeton ha utilizzato anche un Ipod per effettuare il dump della memoria, caricando al suo interno i programmi necessarie per poter estrarre i dati oggetto dell'attacco cold boot.





Anche il famoso programma per la protezione dei dati di Apple Filevault è risultato vulnerabile agli attacchi cold boot e inoltre username e password sono stati ritrovati varie volte all'interno della memoria ram.

Controllo remoto

Visualizzare il desktop del nostro PC da un'altra postazione, avviare e chiudere programmi, scambiare file: Teamviewer fa tutto questo e molto altro

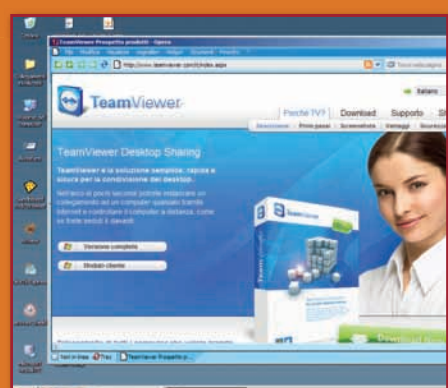


Quante volte ci capita di pensare al computer di casa quando ce ne separiamo momentaneamente, magari mentre siamo al lavoro? Un file che abbiamo dimenticato di trasferire sulla chiavetta USB e che ci servirebbe proprio ora, una sessione di eMule lasciata attiva per un download di grandi dimensioni, un'email scaricata col client di posta e non più reperibile sul server: sono queste le circostanze più comuni in cui ne avvertiamo la mancanza. Servirebbe un software che con un clic faccia apparire sul monitor, come per magia, il desktop del nostro PC. Per fortuna questo programma esiste e si chiama Teamviewer, www.teamviewer.com.

:: Facilissimo

Teamviewer promette estrema semplicità di utilizzo, ricchezza di funzioni, licenza gratuita, almeno per usi non commerciali.

Al primo avvio del programma, però, ci rendiamo conto che la realtà è ancora più entusiasmante. Il software genera immediatamente un ID e una password che serviranno come identificativo per raggiungere il PC di casa via Internet. Annotiamoli, lasciamo attivo Teamviewer e avviamolo sulla macchina da cui ci connetteremo in remoto. A questo punto è sufficiente inserire i dati del computer da controllare e siamo pienamente operativi, col desktop remoto in bella vista sul nostro monitor e



▲ Teamviewer è gratuito per uso personale ed è disponibile anche in una versione compatibile con il sistema operativo Mac OS X. Possiamo quindi controllare anche un Apple.

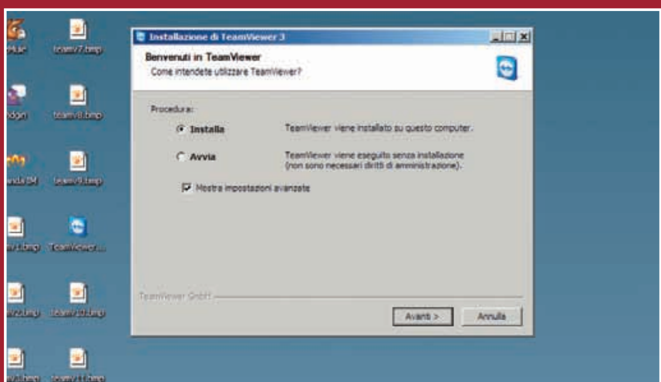
collegamenti, programmi e file di nuovo a completa disposizione.

:: Doppio modulo

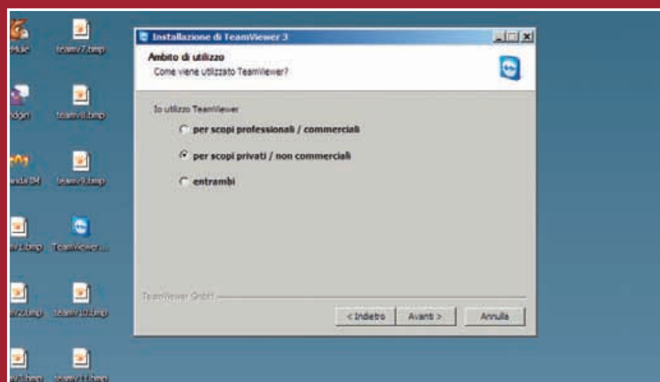
La pagina principale del sito offre due diversie modalità di download. Il primo, indicato come Versione completa, consente sia di controllare un computer, sia di abilitare il controllo del nostro PC da parte di terzi, mentre il Modulo utente si limita a supportare la seconda modalità, ovvero quella passiva.

In linea di massima, è consigliabile tenere la prima versione nella nostra "cassetta degli attrezzi" per sfruttarne la maggiore ricchezza di funzioni. In ogni caso, il secondo modulo, che genera immediatamente i dati per l'identificazione del computer remoto, richiede solo pochi clic del mouse in più per arrivare allo stesso risultato. Già in sede di installazione possiamo apprezzare la versatilità di Teamviewer, che offre la possibilità di procedere al semplice avvio senza che sia necessairo scrivere nulla sul disco fisso o nel Registro di Windows. L'installazione completa è necessaria se pensiamo di farne uso con maggiore frequenza e ci consente di sfruttare alcune impostazioni utili, per esempio quella che prevede l'avvio automatico del programma all'accensione del PC in modo che il computer sia raggiungibile ancor prima di avere effettuato l'accesso come utente. In quest'ultimo caso, ricordiamoci di sostituire le brevissime serie alfanumeriche generate in automatico con una password più lun-

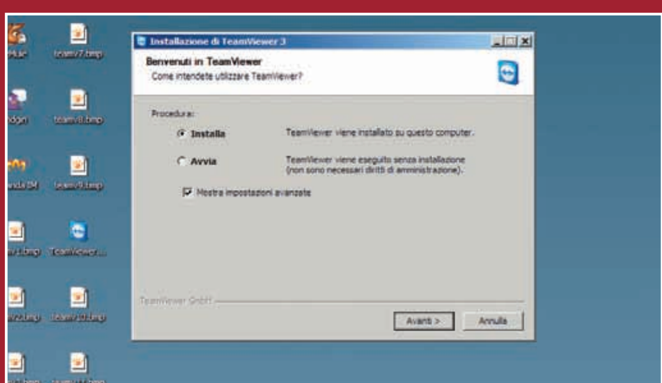
LANCIAMO UNA SESSIONE DI TEAMVIEWER



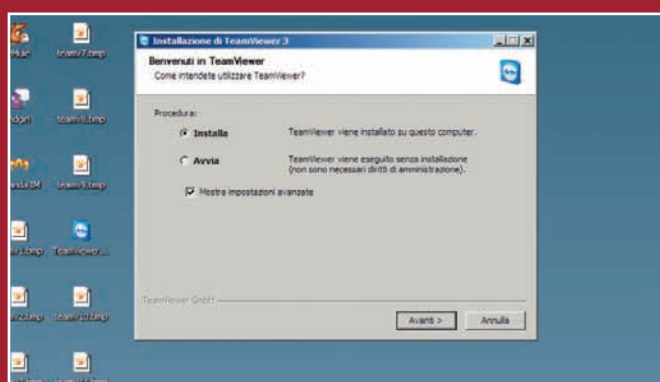
SENZA INSTALLAZIONE
Il programma offre l'alternativa fra un'installazione completa e il semplice avvio senza "sporcare" il Registro di Windows. Le impostazioni avanzate, però, sono disponibili solo nel primo caso.



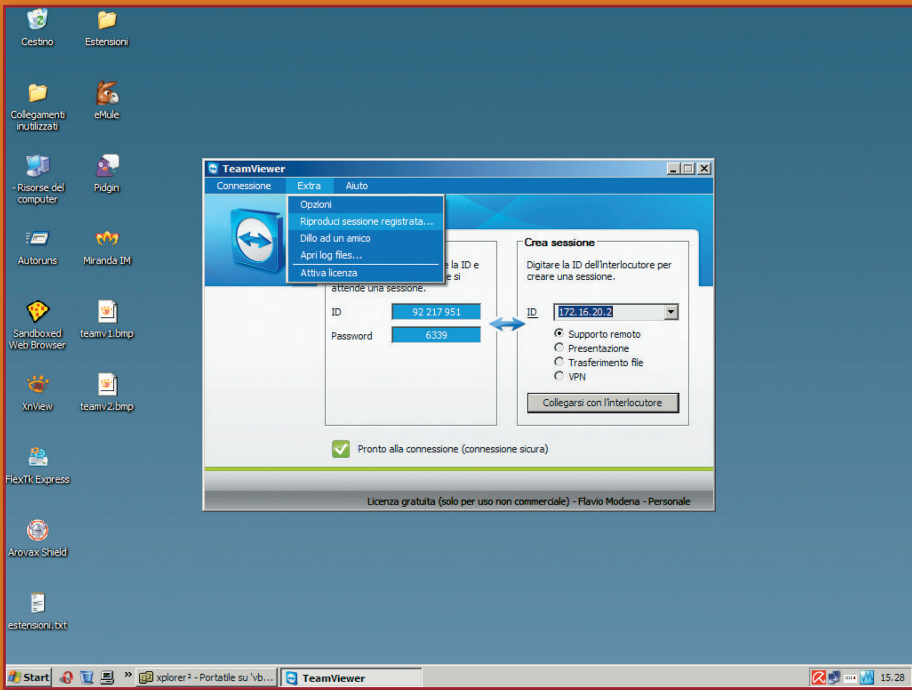
SOLO PER PRIVATI
Il successivo ventaglio di opzioni non ha una valenza tecnica, ma riguarda la licenza. L'utilizzo gratuito del programma è infatti limitato agli scopi privati / non commerciali o comunque senza fine di lucro. Un avvertimento importante.



VPN? NON SERVE
Subito dopo, Teamviewer offre l'integrazione delle funzionalità di VPN, Virtual Private Network. Si tratta di una funzione che serve solo in casi particolari. Se non ci serve è meglio evitare di aggiungere il segno di spunta.



ID E PASSWORD
Con la generazione di ID e Password siamo pronti per metterci al lavoro. La modalità descritta vale sia per il PC controllore che per quello controllato: il titolare di quest'ultimo dovrà solo comunicare all'altro i dati per il collegamento.



Oltre al controllo remoto, abbiamo a disposizione la funzione VPN e la visualizzazione del monitor sul display del computer controllato: l'ideale per una Presentazione.

ga, usando anche lettere maiuscole, numeri o caratteri speciali. Lasciare una password "debole", in questo caso, sarebbe una leggerezza imperdonabile.

:: Nessuna configurazione

La facilità d'uso che caratterizza Teamviewer emerge anche da altri dettagli. Primo fra tutti, la possibilità di avviarlo come utente senza privilegi di amministrazione. Sembra un dettaglio, ma diventa una caratteristica di fondamentale importanza se vogliamo usare il programma all'interno di una rete aziendale. Molto spesso, infatti, le macchine che funzionano in questo contesto vengono limitate per impedire che siano installati programmi "estranei" al lavoro.
Anche la disponibilità di banda non costituisce un problema. Teamviewer, infatti, integra un sistema che ottimizza automaticamente il traffico dei dati in rapporto alla connettività disponibile. La cifratura dei dati in transito, inoltre, ci mette al riparo dalle ipotesi di intrusione da parte di ospiti indesiderati, mentre il sistema automatico per la ricerca delle porte libere su cui operare rende superfluo qualsiasi intervento manuale su router e firewall.

;; Per vederci chiaro

Le doti di Teamviewer non si esauriscono nell'immediatezza del suo utilizzo. Al suo interno troviamo anche un'ottima dotazione di funzioni e opzioni aggiuntive che si rivelano estremamente utili nel corso dell'uso.
Uno sfondo del desktop poco uniforme, per esempio, rischia di pregiudicare la visibilità di icone e finestre nell'immagine. Quando controlliamo a distanza un PC con Teamviewer, infatti, l'immagine del desktop è meno nitida dell'originale. Per evitare che questa perdita di qualità si trasformi in un problema, il menu Visualizza ci consente di rimuovere l'immagine di sfondo, chiamata nel menu con la strana definizione di Carta da parati, sostituendola con un semplice blu uniforme. In questo modo abbiamo a disposizione uno sfondo più adatto ad evidenziare il contenuto della "scrivania".
Un discorso simile vale per la possibilità di mettere a fuoco una singola finestra del desktop remoto, dedicandole l'intero spazio a disposizione. In qualsiasi momento possiamo poi ritornare, sempre in punta di clic, alla visualizzazione dell'intero desktop. La visualizzazione è disponibile in scala, nelle dimensioni originali o a tutto schermo, permettendoci così di aggirare eventuali problemi di compatibilità fra monitor con differenti risoluzioni native.

:: Vado al massimo

Alcuni strumenti integrati nel programma sono pensati per l'uso in un contesto più complesso. È bene ricordare, infatti, che il programma è disponibile anche in versione a pagamento per un uso commerciale. Tra questi c'è, per esempio, la possibilità di usare Teamviewer per creare una VPN, ovvero una Virtual Private Network che permette di creare un collegamento tra computer situati in luoghi diversi e farli comunicare come se fossero in una rete locale. Il collegamento è protetto dallo stesso sistema di cifratura con crittografia AES a 256 bit utilizzato per il controllo remoto e offre quindi un ottimo livello di sicurezza.
Se entrambi i PC sfruttano la versione completa, inoltre, è possibile effettuare lo scambio di ruoli. Il controllato diventa controllore e viceversa. Tutto avviene in tempo reale e l'intera procedura può essere controllata con il solo uso del mouse.
Le versioni più recenti hanno introdotto anche un sistema di registrazione della sessione di lavoro: quanto accade sul desktop remoto viene registrato e trasformato in un filmato. Il tutto viene memorizzato nell'inconsueto formato .TVS, che possiamo visualizzare usando lo stesso Teamviewer. La registrazione può essere avviata, sospesa, ripresa o terminata in qualsiasi momento nel corso della sessione.

:: Non solo controllo

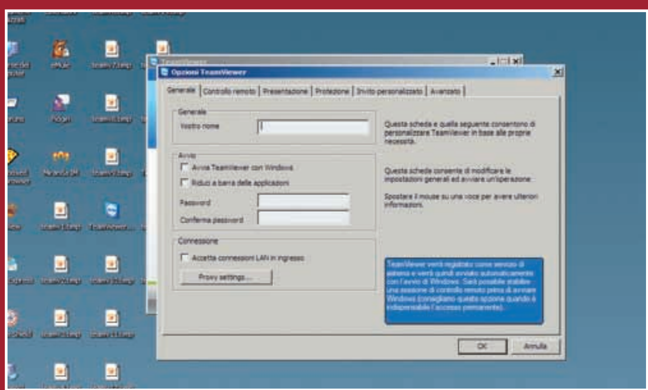
Sin qui abbiamo dato per scontato che questa piccola, ma utilissima applicazione venga sfruttata per il controllo remoto. Non si tratta, però,

dell'unica modalità di utilizzo a nostra disposizione. La funzione che consente lo scambio dei file, per esempio, può godere di una certa autonomia. Il trasferimento, infatti, è avviabile sia autonomamente, sia all'interno di una sessione di controllo remoto. Interessante anche la Presentazione, che permette di visualizzare il proprio desktop sul monitor del computer controllato. Che si tratti di materiale lavorativo o filmati delle vacanze, mostrare contenuti a distanza con Teamviewer diventa un'operazione elementare, oltre che dalle potenzialità ancora inesplorate. Ciliegina sulla torta, il programma integra un piccolo ma efficiente client di Chat che completa le modalità di comunicazione fra i due computer, aggiungendo così la possibilità di scambiare messaggi testuali e collaborare con la massima efficacia quando si condivide una sessione.

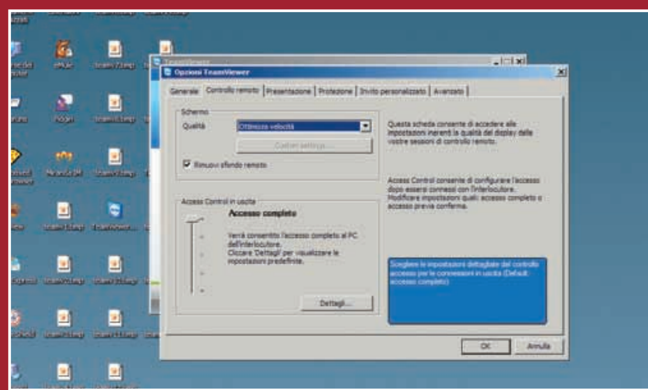
:: Multipiattaforma

Sul sito di Teamviewer è presente anche una versione del programma per computer Mac. A prima vista non sembra una grande notizia, ma le cose cambiano se consideriamo che il programma consente il funzionamento anche tra piattaforme differenti. Grazie a questa caratteristica, quindi, possiamo controllare a distanza un computer con sistema operativo Apple dal nostro PC. Il supporto multipiattaforma risulta utile anche se dobbiamo scambiare o condividere file, un'operazione che in rete locale causa sempre qualche problema.

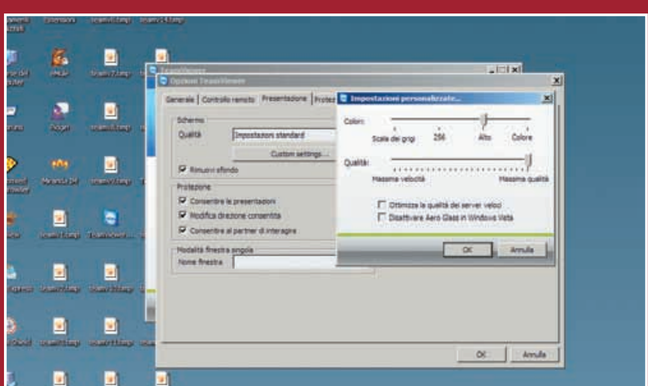
CONFIGURIAMO LE OPZIONI AVANZATE



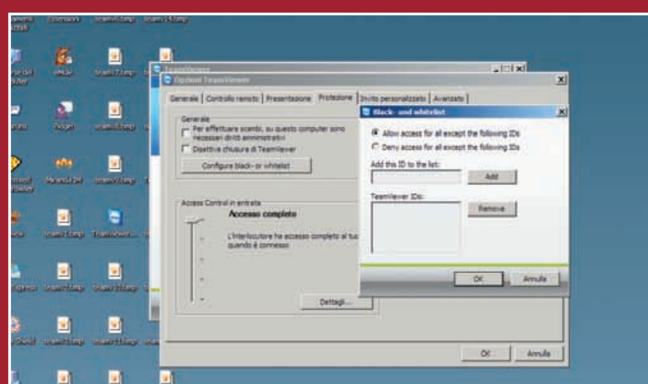
AVVIO AUTOMATICO
La sezione Generale delle Opzioni, accessibile dal menu Extra, include l'avvio automatico con Windows, come applicazione o come servizio di sistema. Utile se usiamo spesso il programma e non vogliamo procedere all'avvio manuale.



PERMESSI E QUALITÀ DEL DISPLAY
Da Controllo Remoto definiamo le azioni consentite a chi accede da un altro PC. L'altra opzione permette di scegliere fra una maggiore velocità di connessione e una migliore qualità nella visualizzazione del display remoto.



GRAFICA, VIA IL SUPERFLUO
Spostandoci sotto Presentazione abilitiamo, oltre a quest'ultima, lo scambio di ruoli e l'interazione fra i due utenti sul PC controllato. La rimozione dello sfondo desktop migliora la visibilità del display remoto.



PRIVILEGI
Se usiamo frequentemente il programma, è consigliabile creare delle regole di Protezione, per esempio creando una lista di ID per i computer a cui consentire o vietare la connessione. Eviteremo che un intruso sfrutti il software per fare breccia nel PC.

LEGGENDE URBANE

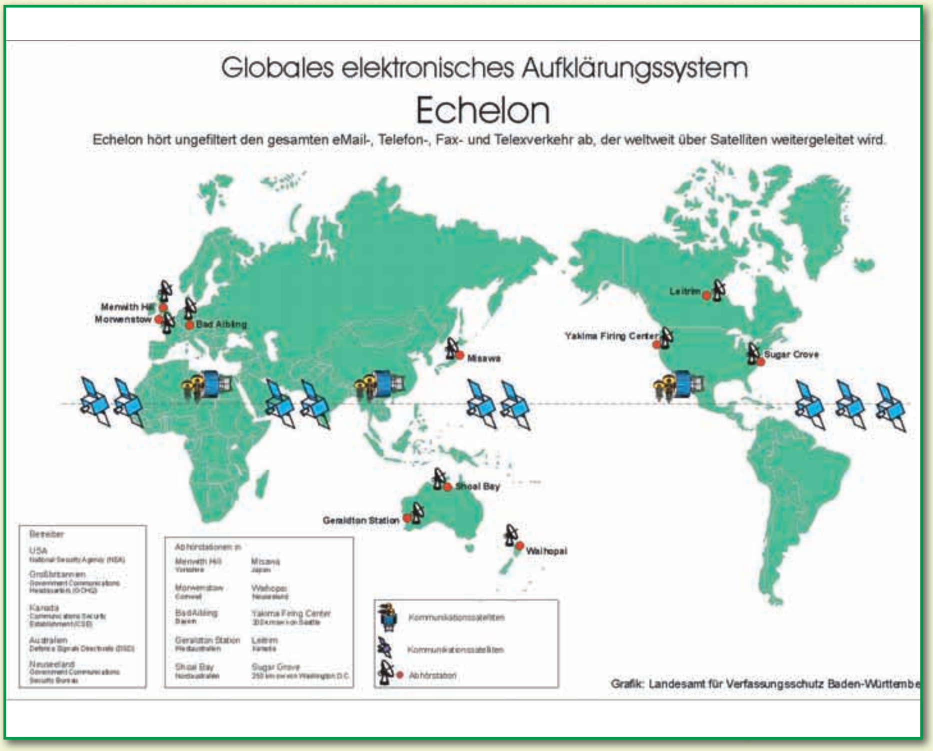
Una guida completa per sopravvivere alle piccole e grandi bufale legate a Internet e all'informatica

Una volta c'erano i tronchetti della felicità invasi dalle micidiali vedove nere. Adesso le leggende metropolitane spopolano in tutti gli ambiti della vita quotidiana e non risparmiano computer, cellulari e qualsiasi altro tipo di apparecchiatura elettronica. Per questo motivo, le cosiddette bufale informatiche sono diventate sempre più complesse e difficili da riconoscere. Dietro a questo tipo di notizie, il più delle volte, c'è solo la fantasia goliardica di qualche buontempone. In alcuni casi, però, ci si possono trovare anche delle mezze verità. Un motivo in più per imparare a riconoscerle e soprattutto, per sapere quando esiste un reale motivo di preoccupazione.

:: Scientificamente discutibile

Fra le tante leggende che circolano in ambito informatico, una delle più discusse non riguarda direttamente i computer, ma addirittura delle piante: un cactus, per la precisione. Secondo alcune voci, infatti, i cactus sarebbero in grado di assorbire l'elettromagnetismo dei nostri PC e quindi, di salvaguardare la nostra salute.
Alla base di tutto c'è un dato di fatto incontrovertibile: l'inquinamento elettromagnetico, così come la radioattività, pur non essendo visibile a "occhio nudo" esiste realmente. Mentre la radioattività è facilmente rilevabile e causa mortalità in tempi ristretti, i reali effetti dell'elettromagnetismo sul corpo umano non sono ancora stati ampiamente e sufficientemente documentati. Negli ultimi





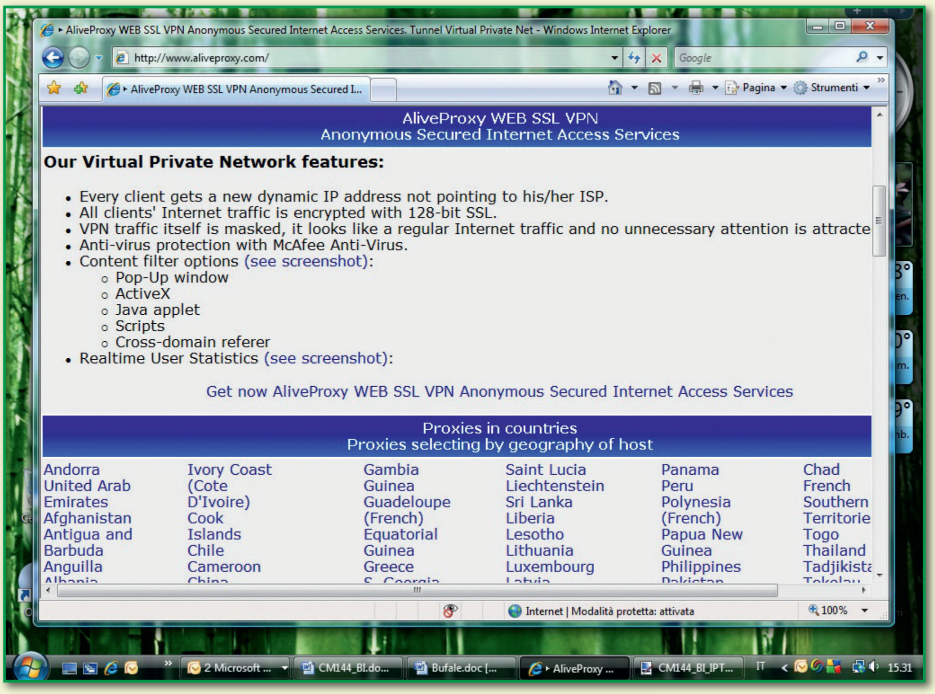
anni alcune ricerche in ambito biofisico hanno però permesso di stabilire dei criteri oggettivi tramite i quali valutare lo stato di salute dell'uomo in relazione alla presenza o meno di campi elettromagnetici.
Lo strumento utilizzato per queste rivelazioni è il biometro di Bovis, un misuratore di energia vitale sulla cui validità la comunità scientifica è attualmente ancora divisa. Nell'ultimo congresso dell'OMS, l'Organizzazione Mondiale per la Sanità, in particolare, questi studi sono stati ripresi e discussi da scienziati di chiara fama come l'ing. Bergsman e altri.

:: Vivere fra le onde

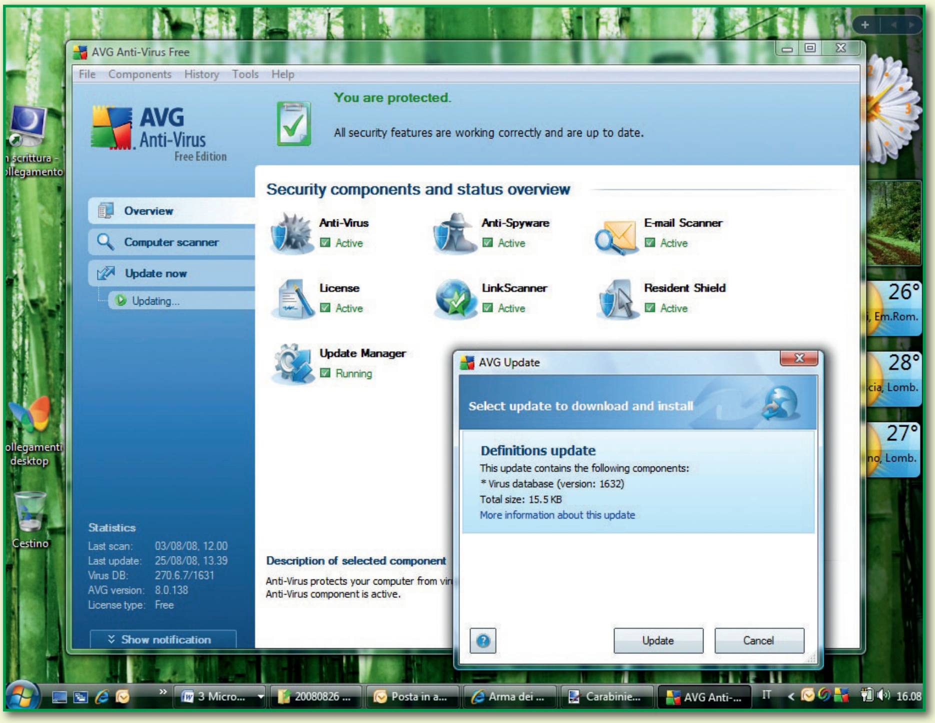
Il principio sul quale si basa lo studio delle interazioni fra i campi elettromagnetici e l'uomo è legato al principio che tutto ciò che è vivo emette vibrazioni misurabili in Amstrong, ovvero della lunghezza d'onda di un dieci milionesimo di millimetro.
L'uomo, in particolare, se si trova in uno stato di buona salute emette circa 6.500 Amstrong. Un'emissione inferiore, invece, corrisponde a uno stato di "sofferenza" o di malattia. Sono state effettuate misure con il biometro di Bovis in migliaia di studi, abitazioni e luoghi pubblici e si è riscontrato che, in presenza di apparecchiature elettromagnetiche accese e funzionanti, il valore iniziale di circa 8.000 Amstrong scendeva di media a circa 3.000 unità. Cioè si veniva a creare uno stato di alterazione dell'equilibrio elettromagnetico avvertibile anche dall'uomo. Ulteriori studi hanno dimostrato, sempre tramite lo stesso principio, che la collocazione di un cactus all'interno dei medesimi ambienti ristabiliva il valore di vibrazioni iniziali.
Al momento, però, non tutti i cactus sembrano avere questa particolare proprietà e l'unica specie per la quale si abbiano riscontri effettivi è quella del Cereus Peruvianus, una specie originaria dei deserti del centro e sud America.

:: Informatica e miti

Un caso limite è rappresentato dal tentativo di "piegare" le Sacre Scritture o altri testi religiosi e civili, per dare sostegno a bufale altrimenti inverosimili. Tempo fa si è diffusa la voce che il codice ASCII del nome di Bill Gates corrispondesse a 666. Cioè, al numero dell'anticristo scritto nel libro dell'Apocalisse.
Per scoprire se le cose stiano realmente in questo modo, basta non lasciarsi tentare dalle simpatie personali e fare qualche piccolo calcolo. La sigla ASCII, infatti, è composta dalle iniziali delle



Ottenere la completa anonimità su Internet è praticamente impossibile e cercare di farlo ricorrendo a mezzi dichiaratamente illegali è perseguibile dalla legge italiana tramite la Polizia Postale.



parole American Standard Code for Information Interchange, ovvero: Standard americano per lo scambio di informazioni.
Un codice ASCII, quindi, è semplicemente la rappresentazione numerica di un qualsiasi carattere di testo espresso dal computer. Dove, per carattere, si intendono sia i "segni speciali", sia le cifre sia infine, le lettere con la distinzione fra maiuscole e minuscole.

:: Verifica immediata

Alcuni elementi del codice ASCII, come il valore "10" o il numero "127", non corrispondono a dei caratteri di testo ma a delle azioni che devono essere eseguite dal computer. Nel caso specifico, rispettivamente, ai comandi vai a capo e cancella.

Per sapere se effettivamente il nome di Bill Gates corrisponde al numero della Bestia della Bibbia, basta, quindi, sostituire a ciascuna lettera il rispettivo valore nel codice ASCII e poi sommarli fra loro. Eccoli uno per uno: B corrisponde a "66", i a "105" mentre ogni l, a "108". Il nome, quindi, vale in totale "387". Se poi sommiamo anche i valori del cognome otteniamo: G, "71"; a, "97"; t, "116"; e, "101"; s, "115". Ovvero "500".In totale, quindi, nome e cognome fanno "887" e del fantomatico "666" non ce n'è traccia. Anche senza usare la sequenza maiuscolo, minuscolo e sommando solo i valori corrispondenti alle lettere maiuscole, che nel codice ASCII hanno valori inferiori, otteniamo il numero "663" che, nuovamente, non è "666".

:: L'uno contro l'altro

Spesso le leggende metropolitane informatiche nascono anche per partito preso: è il caso, per esempio, di coloro che hanno cercato, in passato, di "arginare" la diffusione dei computer a marchio Apple.

La diceria che afferma che i computer Mac sono utili solo per chi fa video o audio editing si è sviluppata agli albori della suddivisione informatica fra chi utilizzava i PC-IBM compatibili e quindi installava i sistemi operativi Microsoft, e quelli che, invece, prediligevano i sistemi Apple. Non era solo una questione di preferenze, molto spesso si trattava esclusivamente di una scelta economica: i computer Apple, infatti, avevano un prezzo molto maggiore dei loro concorrenti a fronte di componenti interne di qualità e di configurazioni più "spinte". Proprio per quest'ultimo motivo, inoltre, erano preferiti dalle aziende che necessitavano di macchine in grado di gestire grandi quantità di dati come, per l'appunto, imprese grafiche o studi musicali.
Nel tempo, l'abbassamento dei prezzi dei componenti e la diffusione di programmi non professionali dedicati alla gestione delle immagini e dei brani musicali, ha trasformato l'originale motivazione in una diceria senza senso. Attualmente, infatti, i computer Mac vanno bene per qualsiasi esigenza e possono essere utilizzati tranquillamente sia nell'ambito delle applicazioni da ufficio sia in quello dei videogiochi.

:: La coperta di Linux

Quando si parla di completa non rintracciabilità delle attività compiute su Internet più che di leggenda metropolitana si tratta di un falso mito diffuso per svariati motivi



Byte	Cod	Char	Byte	Cod	Char	Byte	Cod	Char	Byte	Cod	Char
00000000	0	Null	00100000	32	Spc	01000000	64	@	01100000	96	`
00000001	1	Start of heading	00100001	33	!	01000001	65	A	01100001	97	a
00000010	2	Start of text	00100010	34	"	01000010	66	B	01100010	98	b
00000011	3	End of text	00100011	35	#	01000011	67	C	01100011	99	c
00000100	4	End of transmit	00100100	36	$	01000100	68	D	01100100	100	d
00000101	5	Enquiry	00100101	37	%	01000101	69	E	01100101	101	e
00000110	6	Acknowledge	00100110	38	&	01000110	70	F	01100110	102	f
00000111	7	Audible bell	00100111	39	'	01000111	71	G	01100111	103	g
00001000	8	Backspace	00101000	40	(	01001000	72	H	01101000	104	h
00001001	9	Horizontal tab	00101001	41	)	01001001	73	I	01101001	105	i
00001010	10	Line feed	00101010	42	*	01001010	74	J	01101010	106	j
00001011	11	Vertical tab	00101011	43	+	01001011	75	K	01101011	107	k
00001100	12	Form Feed	00101100	44	,	01001100	76	L	01101100	108	l
00001101	13	Carriage return	00101101	45	-	01001101	77	M	01101101	109	m
00001110	14	Shift out	00101110	46	.	01001110	78	N	01101110	110	n
00001111	15	Shift in	00101111	47	/	01001111	79	O	01101111	111	o
00010000	16	Data link escape	00110000	48	0	01010000	80	P	01110000	112	p
00010001	17	Device control 1	00110001	49	1	01010001	81	Q	01110001	113	q
00010010	18	Device control 2	00110010	50	2	01010010	82	R	01110010	114	r
00010011	19	Device control 3	00110011	51	3	01010011	83	S	01110011	115	s
00010100	20	Device control 4	00110100	52	4	01010100	84	T	01110100	116	t
00010101	21	Neg. acknowledge	00110101	53	5	01010101	85	U	01110101	117	u
00010110	22	Synchronous idle	00110110	54	6	01010110	86	V	01110110	118	v
00010111	23	End trans. block	00110111	55	7	01010111	87	W	01110111	119	w
00011000	24	Cancel	00111000	56	8	01011000	88	X	01111000	120	x
00011001	25	End of medium	00111001	57	9	01011001	89	Y	01111001	121	y
00011010	26	Substitution	00111010	58	:	01011010	90	Z	01111010	122	z
00011011	27	Escape	00111011	59	;	01011011	91	[	01111011	123	{
00011100	28	File separator	00111100	60	<	01011100	92	\	01111100	124	|
00011101	29	Group separator	00111101	61	=	01011101	93	]	01111101	125	}
00011110	30	Record Separator	00111110	62	>	01011110	94	^	01111110	126	~
00011111	31	Unit separator	00111111	63	?	01011111	95		01111111	127	Del

e da più fonti differenti.
Essere sempre e perennemente anonimi è praticamente impossibile. Quello che si può fare è nascondere temporaneamente il nostro IP, cioè l'indirizzo Internet associato al nostro PC, utilizzando un Proxy Server: un computer che si frappone fra noi e la Rete. L'uso di un proxy server consente di inoltrare tutte le nostre richieste Web tramite l'indirizzo IP di quest'ultimo mantenendo così invisibile quello del PC dal quale stiamo lavorando. Si tratta comunque di una soluzione, oltre che limitata nel tempo, non sicura al cento per cento: i proxy server, infatti, spesso smettono di funzionare improvvisamente oppure vengono "traslocati" senza preavviso da un indirizzo a un altro. Per navigare in Rete sfruttando questa possibilità dobbiamo configurare il nostro browser e impostare nella scheda Impostazioni LAN della finestra Connessioni di Rete l'indirizzo IP del Proxy server che vogliamo utilizzare e il relativo numero di Porta.
Questi dati possono essere recuperati su siti specializzati come Alive Proxy: www.aliveproxy.com. Esistono anche alcuni programmi gratuiti, sempre disponibili su Internet, che si preoccupano di applicare le modifiche alla configurazione del nostro browser in automatico.



:: Quasi vere

Le bufale informatiche non risparmiano alcun ambito dell'informatica né, tantomeno, la posta elettronica. A fianco di leggende metropolitane palesemente false esistono però anche mezze verità come quella descritta anche su Wintricks.it, all'indirizzo http://www.wintricks.it/recensioni/virus-no.html
Secondo quanto riportato, scrivere "!000" all'interno della rubrica degli indirizzi permetterebbe di difendersi dai virus. In effetti questa affermazione si basa su un principio che, fino a qualche tempo fa, poteva essere ancora considerato valido: cioè che i virus si auto diffondano infettando la rubrica degli indirizzi a partire dal primo contatto inserito. Purtroppo, però, attualmente non è più così. Esistono infatti molti tipi di worm, come il famigerato Navidad, che agganciano gli indirizzi email dei nostri contatti direttamente dal testo dei messaggi inviati evitando quindi di sfruttare la rubrica.
In conclusione, quindi, pur non trattandosi di un falso, l'utilità di questo trucco rimane legata ai virus di vecchia generazione. Per evitare di contaminare la nostra rubrica dei contatti è necessario sempre installare un buon anti virus e soprattutto evitare di aprire o di leggere qualsiasi messaggio sospetto. ■

